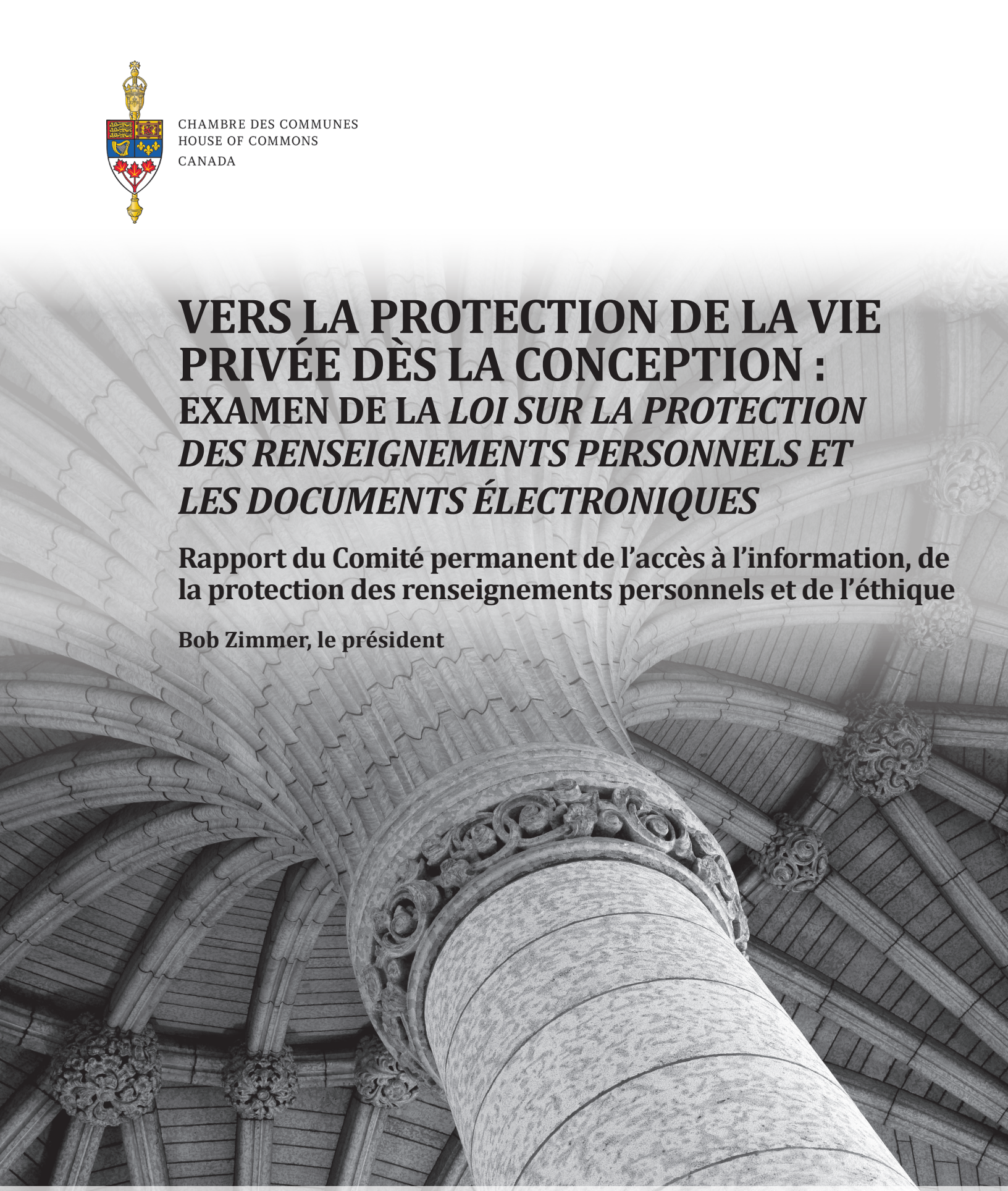
CHAMBRE DES COMMUNES
HOUSE OF COMMONS
CANADA

VERS LA PROTECTION DE LA VIE PRIVÉE DÈS LA CONCEPTION : EXAMEN DE LA *LOI SUR LA PROTECTION DES RENSEIGNEMENTS PERSONNELS ET LES DOCUMENTS ÉLECTRONIQUES*

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

Bob Zimmer, le président



FÉVRIER 2018
42e LÉGISLATURE, PREMIÈRE SESSION

VERS LA PROTECTION DE LA VIE PRIVÉE DÈS LA CONCEPTION : EXAMEN DE LA *LOI SUR LA PROTECTION DES RENSEIGNEMENTS PERSONNELS ET LES DOCUMENTS ÉLECTRONIQUES*

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

Le président
Bob Zimmer

FÉVRIER 2018

42e LÉGISLATURE, PREMIÈRE SESSION

AVIS AU LECTEUR

Rapports de comités présentés à la Chambre des communes

C'est en déposant un rapport à la Chambre des communes qu'un comité rend publiques ses conclusions et recommandations sur un sujet particulier. Les rapports de fond portant sur une question particulière contiennent un sommaire des témoignages entendus, les recommandations formulées par le comité et les motifs à l'appui de ces recommandations.

Pour guider le lecteur :
Un glossaire des termes utilisés dans ce rapport est disponible à la page 97

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

PRÉSIDENT

Bob Zimmer

VICE-PRÉSIDENTS

Nathaniel Erskine-Smith

Charlie Angus

MEMBRES

Frank Baylis	Joyce Murray∗
Mona Fortier	Michel Picard
Jacques Gourde	Raj Saini
L'hon. Peter Kent	Anita Vandenbeld

AUTRES DÉPUTÉS QUI ONT PARTICIPÉ

Vance Badawey	Peter Fonseca	Dan Ruimy
Daniel Blaikie	Matt Jeneroux	Don Rusnak
Bob Bratina	Pat Kelly	Francis Scarpaleggia
Blaine Calkins	Alaina Lockhart	Sonia Sidhu
François Choquette	Wayne Long	Marwan Tabbara
Nathan Cullen	Alistair MacGregor	Karine Trudel
Emmanuel Dubourg	Brian Masse	Len Webber
Ali Ehsassi	Rémi Massé	Erin Weir
Neil R. Ellis	Irene Mathyssen	Salma Zahid
Pat Finnigan	Robert-Falcon Ouellette	

∗ Membre sans droit de vote, conformément à l'article 104(5) du Règlement.

GREFFIER DU COMITÉ

Jean-Denis Kusion

Hugues La Rue

BIBLIOTHÈQUE DU PARLEMENT

Service d'information et de recherche parlementaires

Michael Dewing

Chloé Forget

Marc-André Roy

Alexandra Savoie

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

DOUZIÈME RAPPORT

Conformément au mandat que lui confère l’article 108(3)*h*)(vi)du Règlement, le Comité a étudié la *Loi sur la protection des renseignements personnels et les documents électroniques* (LPRPDE) et a convenu de faire rapport de ce qui suit :

TABLE DES MATIÈRES

LISTE DES RECOMMANDATIONS

À l'issue de leurs délibérations, les comités peuvent faire des recommandations à la Chambre des communes ou au gouvernement et les inclure dans leurs rapports. Les recommandations relatives à la présente étude se trouvent énumérées ci-après.

VERS LA PROTECTION DE LA VIE PRIVÉE DÈS LA CONCEPTION : EXAMEN DE LA *LOI SUR LA PROTECTION DES RENSEIGNEMENTS PERSONNELS ET LES DOCUMENTS ÉLECTRONIQUES*

INTRODUCTION

Le 1er novembre 2016, 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) a adopté une motion afin d'entreprendre l'examen de *la Loi sur la protection des renseignements personnels et les documents électroniques* (LPRPDE)[1].

Le Comité a débuté son étude le 14 février 2017 et a tenu 16 réunions publiques. Il a entendu un total de 68 témoins et a reçu 12 mémoires. De plus, le Comité a tenu compte de l'étude sur le consentement menée par le Commissariat à la protection de la vie privée (CPVP). Les constatations et recommandations à ce sujet figurent dans le rapport annuel 2016–2017 du CPVP[2]. Le Comité a aussi tenu compte d'un projet de position du CPVP sur la réputation en ligne publié le 26 janvier 2018[3]. Le commissaire à la protection de la vie privée du Canada, Daniel Therrien, a comparu au début de l'étude, le 16 février 2017, ainsi qu'à la toute fin, le 1er février 2018.

Dans un mémoire soumis au Comité le 2 décembre 2016, le commissaire Therrien a proposé que le Comité se penche sur quatre domaines d'intervention dans le cadre de son étude de la LPRPDE[4] :

1) le consentement valable;

2) la réputation et le respect de la vie privée;

---

1 Chambre des communes, Comité permanent de l'accès à l'information, de la protection des renseignements et de l'éthique (ETHI), *Procès-verbal*, 1re session, 42e législature, 1er novembre 2016.

2 Commissariat à la protection de la vie privée du Canada (CPVP), *Rapport annuel au Parlement 2016-2017*, septembre 2017.

3 CPVP, *Projet de position du Commissariat sur la réputation en ligne*, 26 janvier 2018.

4 ETHI, Mémoire du Commissaire à la protection de la vie privé du Canada, 2 décembre 2016.

3) les pouvoirs d'exécution du commissaire;

4) le caractère adéquat de la LPRPDE par rapport au *Règlement général sur la protection des données* (RGPD) de l'Union européenne (UE), qui entrera en vigueur en mai 2018.

Le présent rapport donne un aperçu de la LPRPDE, aborde chacun des domaines d'intervention proposés par le commissaire et formule des recommandations à l'endroit du gouvernement canadien. Il contient également un compte-rendu de la mission du Comité à Washington, D.C., qui a eu lieu du 2 au 4 octobre 2017.

PARTIE 1 : APERÇU DE LA *LOI SUR LA PROTECTION DES RENSEIGNEMENTS PERSONNELS ET LES DOCUMENTS ÉLECTRONIQUES*

A. Historique de la *Loi sur la protection des renseignements personnels et les documents électroniques*

La LPRPDE a vu le jour après de vastes consultations. Exemple de coopération entre de multiples parties intéressées, un comité formé de représentants des consommateurs, d'entreprises, de pouvoirs publics, de syndicats et de professionnels a mis au point une série de principes de protection de la vie privée qui, en 1996, ont été approuvés comme normes nationales par le Conseil canadien des normes sous le titre *Code type sur la protection des renseignements personnels* (le Code type)[5]. La publication du Code type a été suivie de consultations et de documents de discussion prônant la mise en œuvre de ces principes au moyen d'une loi. L'évolution de la situation internationale concernant la protection des données, notamment dans l'UE, a renforcé l'idée d'adopter une loi sur la protection des renseignements personnels du secteur privé au Canada[6].

5 Miguel Bernal-Castillero, *Les lois fédérales du Canada sur la protection de la vie privée*, publication n° 2007-44-F, Ottawa, Service d'information et de recherche parlementaires, Bibliothèque du Parlement, 1er octobre 2013.

6 En 1995, l'UE a adopté une directive assurant la protection des renseignements personnels tout en permettant leur libre circulation au sein de l'UE. Les dispositions de la Directive sont devenues applicables en 1998. La directive obligeait tous les pays membres à s'y conformer en adoptant une loi sur la protection des données ou en modifiant leur législation existante. L'article 25 de la directive étendait la portée de celle-ci au-delà de l'UE en interdisant aux pays membres (et aux entreprises s'y trouvant) de transférer des renseignements personnels à tout pays non membre dont les lois ne protègent pas assez ces renseignements. Voir Parlement européen, Conseil de l'Union européenne, *Directive 95/46/CE du Parlement européen et du Conseil, du 24 octobre 1995, relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données*, 24 octobre 1995. Veuillez noter que le caractère adéquat de la LPRPDE est abordé plus loin dans ce rapport.

B. Champ d'application de la *Loi sur la protection des renseignements personnels et les documents électroniques*

Adoptée en 2000, la LPRPDE est entrée en vigueur en trois étapes entre 2001 et 2004[7]. Cette *Loi* s'applique à la collecte, à l'usage ou à la communication de renseignements personnels dans le cadre d'activités commerciales par une organisation du secteur privé et par des installations, des ouvrages, des entreprises ou des secteurs d'activité relevant de la compétence fédérale. Elle régit ces activités non seulement au niveau fédéral et dans les territoires, mais aussi dans toutes les provinces, à moins que celles-ci aient adopté une loi semblable obligeant le secteur privé à accorder une protection comparable (on parle alors d'une « loi essentiellement similaire »). À ce jour, le Québec, la Colombie-Britannique, l'Alberta et, dans les questions liées à la santé, l'Ontario, le Nouveau-Brunswick, la Nouvelle-Écosse et Terre-Neuve-et-Labrador ont adopté une loi réputée essentiellement similaire à la LPRPDE[8].

Plus précisément, au moment actuel, la LPRPDE s'applique aux organisations suivantes :

- organisations du secteur privé qui exercent des activités au Canada dans les provinces ou territoires suivants : Île-du-Prince-Édouard, Manitoba, Nouveau-Brunswick, Nouvelle-Écosse, Nunavut, Ontario, Saskatchewan, Terre-Neuve-et-Labrador, Territoires du Nord-Ouest ou Yukon; mais **pas** en ce qui a trait au traitement des renseignements sur les employés;

- organisations du secteur privé qui exercent des activités au Canada s'il y a transfert interprovincial ou international des renseignements personnels recueillis, utilisés ou communiqués; mais **pas** en ce qui a trait au traitement des renseignements sur les employés;

- organisations sous réglementation fédérale qui exercent des activités au Canada, par exemple les banques, les transporteurs aériens, les compagnies de téléphone ou sociétés de radiodiffusion, **y compris** en ce

7 Le 1er janvier 2001, la LPRPDE s'appliquait au secteur privé réglementé par le gouvernement fédéral (c.-à-d. les banques, les télécommunications et le transport interprovincial), puis le 1er janvier 2002, aux renseignements personnels en santé, et enfin, le 1er janvier 2004, à l'ensemble du secteur privé, même aux organisations qui recueillent, utilisent ou communiquent des renseignements personnels dans une province seulement. Les organisations exerçant leur activité dans les Territoires du Nord-Ouest, le Yukon et Nunavut sont considérées comme des entreprises fédérales au sens de la LPRPDE.

8 CPVP, *Lois provinciales réputées essentiellement similaires à la LPRPDE*. « D'autres provinces et territoires ont également promulgué leurs propres lois sur la protection des renseignements personnels sur la santé, mais ces lois n'ont pas été déclarées essentiellement similaires à la LPRPDE. » (CPVP, *Aperçu des lois sur la protection des renseignements personnels au Canada*.)

> qui a trait au traitement des renseignements sur la santé et concernant les employés[9].

La première partie de la LPRPDE concerne la protection des renseignements personnels dans le secteur privé[10]. L'objet de cette *Loi*, selon son article 3, reconnaît le lien entre la nécessité de protéger les renseignements personnels et celle de les utiliser dans un monde de plus en plus dominé par la technologie de l'information :

> La présente partie a pour objet de fixer, dans une ère où la technologie facilite de plus en plus la circulation et l'échange de renseignements, des règles régissant la collecte, l'utilisation et la communication de renseignements personnels d'une manière qui tient compte du droit des individus à la vie privée à l'égard des renseignements personnels qui les concernent et du besoin des organisations de recueillir, d'utiliser ou de communiquer des renseignements personnels à des fins qu'une personne raisonnable estimerait acceptables dans les circonstances[11].

S'appuyant sur le travail réalisé par les parties prenantes dans la rédaction du Code type, la LPRPDE intègre ce dernier dans la législation en exigeant que les organisations assujetties à la LPRPDE se conforment aux exigences qui y sont énoncées. Le Code type est reproduit à l'annexe 1 de la LPRPDE. En d'autres mots, les organisations ont l'obligation de se conformer aux principes se trouvant à l'annexe 1 de la LPRPDE.

C. Le commissaire à la protection de la vie privée du Canada

Le contrôle d'application de la LPRPDE incombe au commissaire à la protection de la vie privée du Canada, qui est habilité à entendre les plaintes du public ou de toute organisation concernant des violations de la *Loi* et à faire enquête sur ces plaintes[12]. Le commissaire a généralement recours à la médiation et à la conciliation pour régler les plaintes. S'il ne dispose pas du pouvoir de rendre des ordonnances définitives à l'égard d'organisations, le commissaire peut assigner des témoins à comparaître devant lui, faire prêter serment et forcer la production de preuves si l'intéressé ne collabore pas. Dans les affaires non résolues, le commissaire peut demander à la Cour fédérale de rendre une ordonnance pour résoudre la question[13].

---

9 CPVP, *Aperçu des lois sur la protection des renseignements personnels au Canada*.

10 La partie 2 de la LPRPDE porte sur les documents électroniques et vise principalement à les assimiler à des documents juridiques et à préciser à quel moment ils ont force de loi au même titre que les versions sur papier.

11 LPRPDE, art. 3.

12 LPRPDE, art. 11.

13 LPRPDE, art. 14 à 17.

En outre, le commissaire a le pouvoir de procéder à la vérification des pratiques d'une organisation en matière de gestion des renseignements personnels, de rendre public tout renseignement concernant ces pratiques si cela est dans l'intérêt public[14] et de coordonner diverses activités avec ses homologues provinciaux, notamment l'élaboration de contrats types portant sur la protection des renseignements personnels recueillis dans les transactions interprovinciales ou internationales[15]. Le commissaire a aussi pour fonction de faire connaître la LPRPDE au grand public[16].

Finalement, le commissaire a le pouvoir de conclure un accord de conformité avec une organisation à la fin de l'examen d'une plainte afin de s'assurer que celle-ci respecte la LPRPDE[17].

> En vertu d'un accord de conformité, une organisation accepte de prendre certaines mesures pour se conformer à la LPRPDE. Le Commissariat ne peut demander à la Cour une audition sous le régime de la LPRPDE et il doit demander la suspension de toute demande en instance devant la Cour faite sous le régime de cette loi.
>
> Toutefois, si l'organisation n'a pas respecté les engagements pris en vertu d'un accord de conformité, le Commissariat peut demander à la Cour une ordonnance enjoignant à l'organisation de se conformer aux conditions de l'accord, ou demander le rétablissement de l'audition sous le régime de la LPRPDE, selon le cas[18].

D. Examen parlementaire de la *Loi sur la protection des renseignements personnels et les documents électroniques* et tentatives de réforme législative

La LPRPDE dispose que sa première partie, qui porte sur la protection de la vie privée et des renseignements personnels, doit faire l'objet d'un examen parlementaire tous les cinq ans. Le rapport du premier examen parlementaire, qui comportait 25 recommandations de modification de la LPRPDE, a été déposé à la Chambre des

14 LPRPDE, art. 18.

15 LPRPDE, art. 23 et 23.1.

16 LPRPDE, art. 24.

17 LPRPDE, art. 17.1.

18 CPVP, *Trousse d'outils de la LPRPDE pour les entreprises*.

communes en mai 2007 par le Comité[19]. Le gouvernement a répondu aux recommandations en octobre 2007[20].

En mai 2010, le ministre de l'Industrie a présenté le projet de loi C-29, Loi modifiant la *Loi sur la protection des renseignements personnels et les documents électroniques*[21]. Ce projet de loi aurait ajouté de nouvelles exceptions aux exigences de consentement, précisé ce qu'il faut entendre par « validité du consentement » et obligé les organisations à déclarer toute atteinte aux mesures de sécurité des données. Le projet de loi est mort au *Feuilleton* à la dissolution de la 40e législature, le 26 mars 2011. Le 29 septembre 2011, le gouvernement a déposé le projet de loi de nouveau avec le numéro C-12 au début de la 41e législature[22]. Le projet de loi n'a pas été débattu à la Chambre des communes avant la prorogation du 13 septembre 2013, date où il est mort au *Feuilleton*.

En plus des projets de loi du gouvernement, Charmaine Borg, députée de Terrebonne-Blainville, a présenté le projet de loi C-475, Loi modifiant la Loi sur la protection des renseignements personnels et documents électroniques (pouvoir de rendre des ordonnances), pendant la 1re session de la 41e législature. Cette mesure d'initiative parlementaire visant à modifier la LPRPDE aurait également imposé des obligations en matière de déclaration des atteintes aux mesures de sécurité et conféré au commissaire à la protection de la vie privée le pouvoir de rendre des ordonnances de conformité[23].

En 2012, le Comité a réalisé une étude sur la protection des renseignements personnels et les médias sociaux. Durant cette étude, il « a entendu une grande diversité de

---

19 Chambre des communes, Comité permanent de l'accès à l'information, de la protection des renseignements personnels et de l'éthique (ETHI), *Examen, prévu par la loi, de la Loi sur la protection des renseignements personnels et les documents électroniques (LPRPDE)*, Quatrième rapport, 1re session, 39e législature, mai 2007.

20 ETHI, *Réponse du gouvernement au Quatrième rapport du Comité permanent de l'accès à l'information, de la protection des renseignements personnels et de l'éthique : Examen, prévu par la loi, de la Loi sur la protection des renseignements personnels et les documents électroniques (LPRPDE)*, 1re session, 39e législature, octobre 2007.

21 Projet de loi C-29, Loi modifiant la Loi sur la protection des renseignements personnels et les documents électroniques, 3e session, 40e législature.

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

23 Projet de loi C-475, Loi modifiant la Loi sur la protection des renseignements personnels et documents électroniques (pouvoir de rendre des ordonnances), 1re session, 41e législature (reporté à la 2e session, 41e législature, rejeté à la deuxième lecture le 29 janvier 2014). Le projet de loi C-475 aurait certes imposé l'obligation de déclarer les atteintes à la sécurité, mais selon une norme et une démarche différentes de celles prévues dans le projet de loi C-29.

témoignages sur le cadre législatif canadien et particulièrement sur la LPRPDE ». Dans son rapport, le Comité précise que :

> 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[24].

Depuis, aucun examen législatif de la LPRPDE n'a eu lieu[25]. Cependant, le 23 mai 2013, le CPVP a présenté son point de vue sur la réforme de la LPRPDE dans un document intitulé *Arguments en faveur de la réforme de la* Loi sur la protection des renseignements personnels et les documents électroniques[26].

Dans ce document, la commissaire de l'époque, Jennifer Stoddart, a recommandé[27] :

- que l'on confère au Commissariat à la protection de la vie privée de plus grands pouvoirs en matière d'application de la loi;
- que l'on oblige les organisations à signaler au Commissariat les atteintes à la protection des renseignements personnels et, lorsqu'il y a lieu, à en informer les personnes touchées;
- que l'on ajoute des exigences de déclaration afin d'accroître la transparence relativement au recours à une exception prévue dans la

---

24 ETHI, *Protection de la vie privée et médias sociaux à l'ère des mégadonnées*, Cinquième rapport, 1re session, 41e législature, avril 2013, p. 37. Un certain nombre de témoins qui ont comparu durant l'étude ont fait des observations sur le projet de loi C-12.

Par exemple, selon Tamir Israel, de la Clinique d'intérêt public et de politique d'Internet du Canada Samuelson-Glushko de l'Université d'Ottawa, 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 » (p. 38).

Jennifer Stoddart, qui était alors commissaire à la protection de la vie privée du Canada, s'était dite inquiète que « dans 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 de données et les bris de confidentialité relatifs aux données » (p. 39). Elle avait suggéré qu'une façon de renforcer la mesure législative serait d'établir 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 » (p. 39).

25 Aux termes de l'article 29 de la LPRPDE, un examen parlementaire aurait dû avoir lieu en 2011–2012 (cinq ans après l'examen précédent).

26 CPVP, *Arguments en faveur de la réforme de la* Loi sur la protection des renseignements personnels et les documents électroniques, 23 mai 2013.

27 Des options possibles sont des dommages-intérêts prévus par la loi administrés par la Cour fédérale, ainsi que le fait de conférer au commissaire à la protection de la vie privée le pouvoir de rendre des ordonnances, d'imposer des pénalités pécuniaires administratives, ou les deux, lorsque les circonstances l'exigent.

LPRPDE permettant aux agences et organismes de l'État d'obtenir des renseignements personnels auprès d'organisations sans le consentement des intéressés pour différentes raisons, notamment la sécurité nationale et le contrôle d'application des lois;

- que l'on modifie la LPRPDE afin de permettre au Commissariat de conclure des « ententes exécutoires » avec des organisations pour faire en sorte qu'elles remplissent leurs engagements à se conformer aux recommandations faites par le Commissariat à l'issue des enquêtes[28].

E. Récentes modifications apportées à la *Loi sur la protection des renseignements personnels et les documents électroniques*

Le projet de loi S-4, *Loi sur la protection des renseignements personnels numériques*, selon son titre abrégé, présenté au Sénat et lu pour la première fois le 8 avril 2014 et amendé par le Comité sénatorial permanent des transports et des communications, a reçu la sanction royale le 18 juin 2015.

Il a modifié la LPRPDE afin, notamment :

- de permettre la communication de renseignements personnels à l'insu de l'intéressé ou sans son consentement dans certaines circonstances;

- d'obliger les organisations à prendre diverses mesures dans les cas d'atteinte à la sécurité des données[29];

- d'ériger en infraction le fait de ne pas remplir ses obligations en cas d'atteinte à la sécurité des données;

28 Comme mentionné plus haut, le commissaire a dorénavant le pouvoir de conclure un accord de conformité avec une organisation à la fin de l'examen d'une plainte afin de s'assurer que celle-ci respecte la LPRPDE. Le projet de loi S-4, Loi modifiant la Loi sur la protection des renseignements personnels et les documents électroniques et une autre loi en conséquence a modifié la LPRPDE en y ajoutant notamment ce pouvoir.

29 Veuillez noter que « les nouvelles exigences de la LPRPDE en cas d'atteinte à la protection des données entreront en vigueur quand le gouvernement aura édicté le règlement, ce qui leur conférera davantage de clarté et de précision ». Voir, Innovation, Sciences et Développement économique Canada, Pour discussion — Règlement sur la notification et la déclaration des atteintes à la protection des données, mars 2016.

- de permettre au commissaire, dans certaines circonstances, de conclure un accord de conformité avec une organisation[30].

Le projet de loi S-4 a repris certaines dispositions du projet de loi C-12. Il semble également avoir donné suite à certaines recommandations formulées par des témoins lors de l'étude sur la protection de la vie privée et les médias sociaux faite par le Comité en 2012, et par l'ex-commissaire Stoddart dans son exposé de principes de mai 2013[31].

Il est à noter que la *Loi canadienne anti-pourriel*[32] (LCAP) a été adoptée en décembre 2010 et elle est entrée en vigueur le 1er juillet 2014, à l'exception des dispositions visant l'installation non sollicitée de programmes d'ordinateur ou de logiciels, qui sont entrées en vigueur le 15 janvier 2015. La LCAP prévoit notamment un droit privé d'action devant les tribunaux, bien que cette partie de la loi ne soit pas encore en vigueur. La LCAP prévoit également l'imposition de sanctions administratives pécuniaires et de sanctions criminelles[33]. La LCAP interdit notamment d'envoyer des messages électroniques commerciaux sans le consentement des destinataires, y compris des messages envoyés à des adresses électroniques, à des comptes de réseaux sociaux et des messages textes à des cellulaires.

En outre, la LCAP a notamment apporté des modifications à la LPRPDE. En vertu de ces nouvelles dispositions, le commissaire partage les responsabilités relatives à l'application de la LCAP avec le Conseil de la radiodiffusion et des télécommunications canadiennes (CRTC) et le Bureau de la concurrence :

> Le CRTC est chargé des enquêtes sur l'envoi de messages électroniques commerciaux non sollicités, la modification de données de transmission et l'installation de logiciels sans consentement.
>
> Le Bureau de la concurrence s'occupe des déclarations fausses ou trompeuses et des pratiques commerciales déloyales dans le cybermarché.
>
> De son côté, le Commissariat se concentre sur deux types d'infractions :

---

30 Dara Lithwick, *Résumé législatif du projet de loi S-4 : Loi modifiant la Loi sur la protection des renseignements personnels et les documents électroniques et une autre loi en conséquence*, publication n° 41-2-S4-F, Ottawa, Service d'information et de recherche parlementaires, Bibliothèque du Parlement, 11 juin 2014.

31 *Ibid*.

32 *Loi visant à promouvoir l'efficacité et la capacité d'adaptation de l'économie canadienne par la réglementation de certaines pratiques qui découragent l'exercice des activités commerciales par voie électronique et modifiant la Loi sur le Conseil de la radiodiffusion et des télécommunications canadiennes, la Loi sur la concurrence, la Loi sur la protection des renseignements personnels et les documents électroniques et la Loi sur les télécommunications*, L.C. 2010, ch. 23.

33 Gouvernement du Canada, La Loi canadienne anti-pourriel, Faits en brefs.

- la collecte d'adresses électroniques, selon laquelle des listes en vrac d'adresses électroniques sont compilées par divers mécanismes dont des programmes informatiques qui fouillent de façon automatique Internet pour y trouver des adresses;

- la collecte de renseignements personnels en accédant aux systèmes informatiques d'autres personnes de manière illicite, principalement au moyen de logiciels espions[34].

F. Enjeux constitutionnels

Comme telle, la protection des renseignements personnels n'est pas une matière explicitement traitée par le partage des compétences prévue dans la *Loi constitutionnelle de 1867*[35]. Il s'agit d'une matière qui comporte des aspects touchant les gouvernements fédéral et provinciaux. Sur le plan fédéral, la LPRPDE a été adoptée par le Parlement du Canada en vertu de sa compétence sur la réglementation du commerce interprovincial, prévue au paragraphe 91(2) de la *Loi constitutionnelle de 1867*. À l'époque, la position du gouvernement fédéral était que les renseignements personnels constituent des biens pouvant faire l'objet d'un commerce et que leur protection est un enjeu transfrontalier nécessitant un encadrement législatif fédéral[36].

Les provinces sont également en mesure de légiférer en matière de protection des renseignements personnels en vertu de leur pouvoir sur les questions liées à la propriété et aux droits civils au titre du paragraphe 92(13) de la *Loi constitutionnelle de 1867*. Il s'agit d'une compétence assez vaste qui permet aux législatures provinciales de légiférer sur les questions de nature privée intraprovinciales, incluant le commerce, les contrats, les relations entre les personnes, etc. Cette compétence permet aux provinces d'adopter des lois visant la protection de la vie privée qui sont analogues à la LPRPDE.

La constitutionnalité de la LPRPDE a été remise en doute à quelques reprises depuis son adoption. Certains soutiennent qu'il s'agit d'une loi fédérale qui régit un domaine exclusivement provincial dans lequel une intervention législative fédérale n'est pas nécessaire ou permissible[37]. En outre, le gouvernement du Québec a, en 2003, initié un

34 CPVP, *Responsabilités incombant au Commissariat en vertu de la LCAP*.

35 *Loi constitutionnelle de 1867*, 30 & 31 Victoria, c. 3.

36 Chambre des Communes, *Hansard*, 36e législature, 2e session, numéro 9 (22 octobre 1999), p. 537.

37 Pour une analyse complète de la question de la constitutionnalité de la LPRPDE, voir Michel Bastarache, *The Constitutionality of PIPEDA: A Re-consideration in the Wake of the Supreme Court of Canada's Reference re Securities Act*, juin 2012. Les deux articles suivants soutiennent que la LPRPDE est constitutionnelle, mais ils ont été publiés avant que la Cour suprême du Canada publie son avis consultatif dans le *Renvoi relatif à la Loi sur les valeurs mobilières*, [2011] 3 RCS 837, 2011 CSC 66 : Mahmud Jamal, « Is PIPEDA Constitutional? », 43 Can. Bus. L.J. 434 (2006); Josh Nisker, « PIPEDA: A Constitutional Analysis », 85 Can. B. Rev. 317 (2006).

renvoi devant la Cour d'appel du Québec afin de déterminer si la LPRPDE empiète de manière inconstitutionnelle sur les champs de compétence provinciaux. Cette procédure judiciaire n'a pas été menée à terme. Dans une autre affaire devant la Cour fédérale, la validité constitutionnelle de la LPRPDE a été soulevée par une partie, mais la Cour a ultimement refusé de trancher la question[38]. La constitutionnalité de la LPRPDE sur le plan du partage des compétences n'a toujours pas été tranchée par les tribunaux.

PARTIE 2 : LE CONSENTEMENT VALABLE SOUS LE RÉGIME DE LA *LOI SUR LA PROTECTION DES RENSEIGNEMENTS PERSONNELS ET LES DOCUMENTS ÉLECTRONIQUES*

A. Le principe général du consentement tel que prévu dans la *Loi sur la protection des renseignements personnels et les documents électroniques*

Le modèle actuel de protection de la vie privée et d'échange de renseignements personnels repose en grande partie sur le principe selon lequel les usagers échangent leurs renseignements personnels pour obtenir des services. Il s'agit essentiellement d'un contrat, qui repose en théorie sur un consentement éclairé des individus qui acceptent de communiquer des renseignements personnels qui les concernent. Comme l'indique Michael Karanicolas, du Centre for Law and Democracy (CLD) :

> La dynamique qui sous-tend [le modèle du consentement] et qui fait tourner une bonne partie de l'économie numérique est le fait que les utilisateurs peuvent choisir d'échanger leurs renseignements personnels contre des services. Ce modèle présente des avantages indéniables, qui a contribué à la croissance rapide d'Internet en faisant baisser les coûts d'entrée. Cependant, cette dynamique repose sur le consentement valable, ce qui signifie que la partie contractante doit avoir une compréhension superficielle de ce qu'elle signe[39].

La prémisse du modèle du consentement est que la meilleure protection des renseignements personnels consiste à s'assurer que chaque personne demeure libre de

38 *State Farm Mutual Automobile Insurance Company c. Commissaire à la protection de la vie privée du Canada et le Procureur général du Canada*, 2010 CF 736.

39 ETHI, *Témoignages*, 1re session, 42e législature, 23 février 2017, 1530 (Michael Karanicolas, conseiller juridique principal, Centre for Law and Democracy).

disposer de ses renseignements personnels comme elle le souhaite, incluant en les échangeant pour des services[40].

Les règles concernant le consentement dans la LPRPDE sont résumées dans les paragraphes qui suivent :

- **Principe général** : Le troisième principe énoncé à l'annexe 1 de la LPRPDE précise les règles applicables au consentement pour la collecte, l'utilisation ou la communication de renseignements personnels. Toute organisation doit se conformer aux obligations qui y sont énoncées[41]. Le principe général en ce qui concerne le consentement est le suivant : « Toute personne doit être informée de toute collecte, utilisation ou communication de renseignements personnels qui la concernent et y consentir, à moins qu'il ne soit pas approprié de le faire[42]. » Il est à noter que la LPRPDE comporte plusieurs exceptions où une organisation pourrait à l'insu d'un individu et sans son consentement, recueillir, utiliser ou communiquer ses renseignements personnels. Par exemple, il pourrait être impossible ou peu réaliste d'obtenir le consentement d'une personne concernée pour des raisons juridiques ou médicales[43].

- **Moment d'obtenir le consentement** : Le consentement de la personne concernée doit être obtenu « avant de recueillir des renseignements personnels à son sujet et d'utiliser ou de communiquer les renseignements recueillis ». Le consentement peut être obtenu au moment de la collecte de renseignements. Le consentement doit également être obtenu lorsqu'une organisation prévoit utiliser des renseignements recueillis à une nouvelle fin.

- **Validité du consentement** : Afin que le consentement soit valable, « les fins doivent être énoncées de façon que la personne puisse raisonnablement comprendre de quelle manière les renseignements seront utilisés ou communiqués[44] ».

---

40 Voir ETHI, *Témoignages*, 1re session, 42e législature, 14 février 2017, 1610 (Éloïse Gratton, associée et cochef nationale, Groupe de pratique Respect de la vie privée et protection des renseignements personnels, Borden Ladner Gervais).

41 LPRPDE, par. 5(1).

42 LPRPDE, annexe 1, « 4.3 Troisième principe, consentement ».

43 *Ibid.*

44 *Ibid.*, 4.3.2.

- **Limite concernant la quantité de renseignements personnels exigés** : « Une organisation ne peut pas, pour le motif qu'elle fournit un bien ou un service, exiger d'une personne qu'elle consente à la collecte, à l'utilisation ou à la communication de renseignements autres que ceux qui sont nécessaires pour réaliser les fins légitimes et explicitement indiquées[45]. »

- **Forme du consentement et la façon de l'obtenir** : La forme du consentement et la façon d'obtenir le consentement peuvent varier selon les circonstances et la nature des renseignements. Les organisations doivent tenir compte de la sensibilité des renseignements. De plus, « dans l'obtention du consentement, les attentes raisonnables de la personne sont aussi pertinentes[46] ». La personne visée « peut retirer son consentement en tout temps, sous réserve de restrictions prévues par une loi ou un contrat et d'un préavis raisonnable. L'organisation doit informer la personne des conséquences d'un tel retrait[47] ».

B. L'avenir du consentement comme principe de base de la *Loi sur la protection des renseignements personnels et les documents électroniques*

Comme l'a expliqué le commissaire, les innovations récentes en matière de technologies de l'information ont mené à une complexification importante des interactions en ligne ainsi qu'à la multiplication des types d'utilisation des renseignements personnels :

> Au moment de l'adoption de la LPRPDE, les interactions avec les entreprises étaient généralement prévisibles, transparentes et bilatérales. Les consommateurs comprenaient bien pourquoi l'entreprise avec laquelle ils faisaient des affaires avait besoin de certains renseignements personnels. Il est maintenant difficile de savoir avec certitude qui traite nos données et, surtout, à quelles fins[48].

Dans ce contexte, plusieurs témoins ont indiqué au Comité que la quantité de renseignements personnels échangés et la fréquence des interactions avec des organisations qui récoltent des renseignements personnels sont telles qu'il est impossible pour les individus de prendre le temps nécessaire de s'informer

45 *Ibid.*, 4.3.3.

46 *Ibid.*, 4.3.5.

47 *Ibid.*, 4.3.8.

48 ETHI, *Témoignages*, 1re session, 42e législature, 16 février 2017, 1530 (Daniel Therrien, commissaire à la protection de la vie privée du Canada).

adéquatement des conditions d'utilisation de chaque service et de donner un consentement réfléchi. Comme l'indique Teresa Scassa, professeure de droit à l'Université d'Ottawa :

> [d]e plus en plus d'appareils que nous avons sur nous et à la maison recueillent et transmettent nos renseignements. Ils peuvent même le faire sans que nous le sachions, et ce de façon continue. Le résultat est qu'il y a bien moins de points ou de moments bien définis où la collecte de données a lieu, ce qui fait en sorte qu'il est difficile de dire qu'un avis a été présenté et qu'un consentement éclairé a été obtenu[49].

Pour Vincent Gogolek, du B.C. Freedom of Information and Privacy Association, le consentement des utilisateurs revêt un caractère illusoire en raison du fait que les conditions d'utilisation sont presque toujours présentées sous la forme de longs et vagues textes juridiques, qui sont à prendre ou à laisser[50]. Les entreprises sont donc facilement en mesure d'obtenir le consentement qu'ils désirent et d'utiliser les renseignements recueillis comme bon leur semble. Le constat, selon Vincent Gautrais, directeur du Centre de recherche en droit public à la Faculté de droit de l'Université de Montréal, est que le consentement s'est transformé d'un outil de protection de l'individu en un « moyen de protéger les entreprises qui l'utilisent [afin de pouvoir] totalement s'affranchir de tout contrat en noyant leurs obligations, leurs manières de faire, dans des pages et des pages[51] ».

De leur côté, des représentants d'entreprises qui œuvrent dans le développement de technologies de l'information ont eux aussi fait valoir au Comité que le modèle du consentement est problématique. Par exemple, Robert Watson, de l'Association canadienne de la technologie de l'information (ACTI), considère que l'exigence de consentement peut ralentir l'innovation et priver les consommateurs de possibilités intéressantes en matière de traitement de données. Ainsi, selon l'ACTI, « ralentir le transfert de l'information nécessaire à la conclusion de transactions pour obtenir le consentement exprès est une pratique qui comporte des limites importantes pour les clients comme pour les entreprises […][52] ». De plus, « [i]l existe aussi des situations où l'utilisation imprévue de données pourrait se révéler très bénéfique pour les utilisateurs,

---

49 ETHI, *Témoignages*, 1re session, 42e législature, 23 février 2017, 1540 (Teresa Scassa, professeure titulaire, Université d'Ottawa, Chaire de recherche du Canada en droit d'information).

50 ETHI, *Témoignages*, 1re session, 42e législature, 16 février 2017, 1640 (Vincent Gogolek, directeur général, B.C. Freedom of Information and Privacy Association).

51 ETHI, *Témoignages*, 1re session, 42e législature, 4 avril 2017, 1640 (Vincent Gautrais, directeur du Centre de recherche en droit public, Faculté de droit de l'Université de Montréal); ETHI, *Témoignages*, 1re session, 42e législature, 23 février 2017, 1540 (Teresa Scassa).

52 ETHI, *Témoignages*, 1re session, 42e législature, 16 mai 2017, 1550 (Robert Watson, président et directeur général, Association canadienne de la technologie de l'information).

mais où il peut être difficile, voire impossible, d'obtenir des expressions de consentement renouvelées[53] ».

Wally Hill, de l'Association canadienne du marketing (ACM) a abondé dans le même sens : « [p]uisque les modèles d'affaires mettent de plus en plus l'accent sur l'innovation et la personnalisation accrue des produits et services, ce que les entreprises font en réaction aux attentes des clients, il faut reconnaître les difficultés que causera un régime axé sur le consentement[54]. »

Bien que la plupart des témoins ayant comparu devant le Comité croient que le consentement, sous une forme ou une autre, devrait demeurer un élément important de la LPRPDE, plusieurs d'entre eux proposent de remédier aux lacunes du modèle actuel en faisant une plus grande place à des éléments de consentement implicites. Selon cette approche, on considère que les individus ont consenti implicitement à la collecte, l'utilisation et la communication de données lorsque le risque de préjudice pour l'utilisateur est faible, voire inexistant[55]. Le consentement serait alors seulement nécessaire lorsqu'il existe un risque de tort à la personne[56]. Cette approche a été décrite brièvement par Éloïse Gratton, associée chez Borden Ladner Gervais (BLG) :

> Par exemple, il faudrait obtenir le consentement express de la personne pour utiliser ses renseignements personnels afin de prendre une décision en matière d'admissibilité qui aurait une incidence sur elle; pour divulguer l'information qui pourrait comprendre des renseignements sensibles ou potentiellement embarrassants; ou pour faire quelque chose qui pourrait aller à l'encontre des attentes de la personne.
>
> L'approche fondée sur le risque permettrait peut-être aux organisations de simplifier leurs communications avec les individus, ce qui réduirait le fardeau imposé aux consommateurs, ainsi que la confusion, puisqu'ils recevraient moins de demandes de consentement. Ainsi, ces demandes voudraient dire quelque chose, parce qu'elles mettraient l'accent sur les questions qui les préoccupent[57].

Le consentement implicite n'est pas complètement étranger au régime actuel. Par exemple, Chantal Bernier, avocate-conseil chez Dentons Canada et ancienne commissaire par intérim et commissaire adjointe à la protection de la vie privée du Canada, a fait remarquer au Comité que l'article 4.3.6 des principes inscrits à l'annexe

---

53 *Ibid.*

54 ETHI, *Témoignages*, 1re session, 42e législature, 11 mai 2017, 1545 (Wally Hill, vice-président, Affaires gouvernementales et des consommateurs, Association canadienne du marketing).

55 ETHI, *Témoignages*, 1re session, 42e législature, 14 février 2017, 1610 (Éloïse Gratton).

56 *Ibid.*

57 *Ibid.*; aussi ETHI, *Témoignages*, 1re session, 42e législature, 11 mai 2017, 1625 (Wally Hill).

de la LPRPDE indique que le consentement implicite peut être jugé suffisant lorsque les renseignements sont moins sensibles[58].

Selon M. Hill, de l'ACM, ce modèle aurait pour effet de transférer une plus grande partie de la responsabilité en matière de protection des renseignements personnels aux entreprises qui les récoltent et ce, en échange d'une plus grande liberté : « il faut imposer aux organisations l'exigence d'évaluer le risque que suppose toute utilisation d'une information, et il faut exiger qu'elles prennent des décisions appropriées en se fondant sur cette évaluation[59]. » Ceci leur permettait de mettre davantage l'accent sur l'innovation et la personnalisation accrue des produits et services. À son avis, un modèle de consentement implicite fondé sur le niveau de risque est compatible avec la notion de consentement et serait avantageux pour le consommateur[60].

Certains témoins ont toutefois mis le Comité en garde quant à la mise en place d'un régime de responsabilité fondé sur le risque. M[me] Scassa craint qu'il soit difficile de bien évaluer les risques en amont :

> Ce qui m'inquiète là-dedans, c'est le seuil voulant qu'il n'y ait aucun risque et aucun préjudice. Je crois que dans le contexte des métadonnées, on tente toujours de déterminer de façon exacte ce que sont ces risques et ces préjudices. Les conséquences de la collecte de certains types de données ne sont pas toujours évidentes dès le départ, et varient selon les renseignements qui sont recueillis et réunis par la suite[61].

Pour Tamir Israel, avocat-conseil à la Clinique d'intérêt public et de politique d'Internet du Canada (CIPPIC), une approche fondée sur le risque pourrait carrément engendrer une « chasse ouverte aux renseignements personnels[62] ». Il indique également que cela minerait grandement la confiance des consommateurs, qui dépend de leur habileté à exprimer un consentement[63].

Un grand nombre de témoins militent plutôt pour le maintien du consentement comme fondement du régime de la LPRPDE et la mise en place de mesures visant à en garantir

---

58 ETHI, *Témoignages*, 1re session, 42e législature, 14 février 2017, 1545 (Chantal Bernier, avocate-conseil, Groupe mondial de la vie privée et cybersécurité, Dentons Canada).

59 ETHI, *Témoignages*, 1re session, 42e législature, 11 mai 2017, 1625 (Wally Hill).

60 *Ibid.*, 1620.

61 ETHI, *Témoignages*, 1re session, 42e législature, 23 février 2017, 1540 (Teresa Scassa).

62 ETHI, *Témoignages*, 1re session, 42e législature, 23 mars 2017, 1630 (Tamir Israel, avocat-conseil à l'interne, Clinique d'intérêt public et de politique d'Internet du Canada).

63 *Ibid.*

la validité[64]. Pour eux, le principe du consentement tel qu'actuellement inscrit dans à LPRPDE est suffisamment rigoureux et flexible pour s'adapter aux problèmes que posent les innovations en matière de technologies de l'information et d'utilisation des renseignements personnels. M[e] Bernier a donné l'exemple de l'article 6.1 de la LPRPDE, qui prévoit que le consentement n'est valable « que s'il est raisonnable de s'attendre à ce qu'un individu visé par les activités de l'organisation 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[65] ». Selon elle, cette disposition appuie l'idée que le principe du consentement actuellement inscrit dans la LPRPDE « prend vraiment en compte la complexité d'Internet, sans toutefois prescrire de modalités, de sorte qu'il est possible d'adapter ce principe à toutes les applications qui se présentent[66] ». Cet avis est partagé par Suzanne Morin, de l'Association du Barreau canadien (ABC), qui a indiqué que le modèle actuel « protège toujours efficacement la vie privée des Canadiens […] en offrant une solution suffisamment souple alors même que les entreprises doivent composer avec l'évolution rapide des technologies, des modèles d'affaires et des attentes des clients en matière de protection de la vie privée[67] ».

Un exemple concret de cette souplesse du régime actuel a été présenté par Adam Kardash, du Bureau de la publicité interactive du Canada (BPI). Ce dernier a expliqué au Comité comment le modèle actuel du consentement est mis en œuvre par l'industrie de la publicité comportementale en ligne. Cette industrie a mis à profit la flexibilité du cadre législatif actuel en créant AdChoices, un « programme canadien d'autoréglementation applicable à la publicité comportementale en ligne » auquel participent des douzaines d'acteurs œuvrant dans ce domaine[68]. M. Kardash a également souligné que la LPRPDE prévoit également des règles utiles applicables à

---

64 Voir notamment ETHI, *Témoignages*, 1re session, 42e législature, 14 février 2017, 1600 (John Lawford, directeur exécutif et avocat général, Centre pour la défense de l'intérêt public); et ETHI, *Témoignages*, 1re session, 42e législature, 30 mai 2017, 1535 (Frank Zinatelli, vice-président et avocat général, Association canadienne des compagnies d'assurances de personnes).

65 ETHI, *Témoignages*, 1re session, 42e législature, 14 février 2017, 1545 (Chantal Bernier).

66 *Ibid.*

67 ETHI, *Témoignages*, 1re session, 42e législature, 23 mars 2017, 1640 (Suzanne Morin, vice-présidente, Section nationale du droit de la vie privée et de l'accès à l'information, Association du Barreau canadien); ETHI, *Témoignages*, 1re session, 42e législature, 4 avril 2017, 1610 (David Young, directeur, David Young Law, à titre personnel).

68 ETHI, *Témoignages*, 1re session, 42e législature, 30 mai 2017, 1600 (Adam Kardash, partenaire, vie privée et gestion de données, Osler, Hoskin et Harcourt S.E.N.R.L., s.r.l., Bureau de la publicité interactive du Canada).

l'analyse et au traitement des mégadonnées à des fins de recherche et de développement[69].

Ainsi, pour plusieurs, le régime actuel de la LPRPDE est fondé sur des principes solides qui sont en mesure de s'adapter aux évolutions technologiques. Plutôt que de remettre en question le modèle du consentement, mieux vaut procéder à des ajustements mineurs et laisser les acteurs – que ce soit le CPVP, les entreprises, le gouvernement, etc. – adapter leurs pratiques afin de maintenir et d'accroître la valeur du consentement.

Le Comité est d'avis que le consentement devrait demeurer au cœur du modèle de protection des renseignements personnels inscrit dans la LPRPDE. En effet, le Comité croit que le respect de l'autonomie individuelle requiert que les individus demeurent généralement libres de choisir par eux-mêmes comment disposer de leurs renseignements personnels. Bien que la multiplication des interactions entre les individus et des entreprises récoltant et échangeant des renseignements personnels ait rendu plus difficile l'obtention d'un réel consentement explicite, le Comité est d'avis que la liberté de choix est un facteur favorisant la confiance chez les consommateurs. Ainsi, plutôt que de délaisser le modèle du consentement, le Comité est d'avis que le gouvernement du Canada devrait chercher à le renforcer et à le clarifier lorsque nécessaire.

Par conséquent, le Comité recommande :

Recommandation 1 sur le principe du consentement :

Que le consentement demeure au cœur du régime de protection des renseignements personnels, mais qu'il soit renforcé et clarifié par des moyens additionnels lorsque possible ou requis.

C. Renforcer le modèle du consentement

Comme l'a indiqué le CPVP dans son rapport annuel 2016–2017, « [l]e consentement demeure au cœur de l'autonomie personnelle, mais il faut ajouter d'autres mécanismes pour l'appuyer et ainsi protéger la vie privée plus efficacement[70] ». Au cours de son étude, le Comité a entendu plusieurs propositions visant à renforcer et clarifier le consentement.

---

69 *Ibid.* Il est à noter que M. Kardash a toutefois indiqué au Comité qu'il pourrait être utile d'apporter une clarification à l'al. 7(2)*c*) de la LPRPDE afin d'indiquer explicitement que *l'analyse* de données à ces fins est permise (non seulement *l'utilisation* des données).

70 CPVP, *Rapport annuel au Parlement 2016-2017*, septembre 2017, p. 20.

1. Les politiques de confidentialité

Un grand nombre de témoins croient qu'il est possible de renforcer considérablement la validité du consentement en améliorant les politiques de confidentialité, qui sont, comme l'indique le CPVP, « le fondement du modèle contractuel de l'avis et du consentement en vigueur[71] ». Pour M[e] Bernier, des politiques de confidentialité améliorées permettraient assez facilement de rendre le consentement moins artificiel :

> [L]'accroissement de la valeur du consentement passe par les politiques de confidentialité. À mon avis, celles-ci doivent satisfaire à trois critères précis. Premièrement, elles doivent être énoncées dans un langage accessible. Deuxièmement, elles doivent être adaptées à l'organisation. Troisièmement, elles doivent être facilement navigables[72].

Abondant dans le même sens, M. Karanicolas, du CLD, croit que les entreprises qui récoltent des renseignements personnels pourraient produire un résumé ou un guide permettant d'expliquer en termes simples leurs ententes de confidentialité, qui sont souvent très longues et rédigées dans un jargon juridique difficile à comprendre. Il croit aussi que des avis clairs devraient être transmis aux utilisateurs lorsque des changements sont apportés[73]. Le CPVP croit aussi que des améliorations aux politiques de confidentialité seraient très bénéfiques et propose d'ailleurs des principes directeurs dans l'étude sur le consentement publiée dans son rapport annuel 2016–2017[74]. De plus, le CPVP indique que les éléments suivants devraient être mis de l'avant dans ces politiques afin d'obtenir un consentement valable :

- Quels renseignements personnels sont recueillis;
- À qui ils sont communiqués, dont une énumération des tiers;
- À quelles fins les renseignements sont recueillis, utilisés ou communiqués, y compris une explication des fins non essentielles à la prestation du service;
- Quel est le risque de préjudice pour l'individu, le cas échéant[75].

---

71 *Ibid.*, p. 23.

72 ETHI, *Témoignages*, 1re session, 42e législature, 14 février 2017, 1545 (Chantal Bernier).

73 ETHI, *Témoignages*, 1re session, 42e législature, 23 février 2017, 1530 (Michael Karanicolas).

74 CPVP, *Rapport annuel au Parlement 2016-2017*, septembre 2017, p. 24.

75 *Ibid.*

Le Comité note cependant que le CPVP, comme organisme de réglementation, ne croit pas avoir un rôle à jouer en matière de rédaction de modèles de politiques de confidentialité[76].

2. L'adhésion facultative

D'autres témoins ont indiqué que le meilleur moyen de combler les lacunes du modèle actuel est de mettre en œuvre un système d'adhésion facultative (*opt in*) par défaut, c'est-à-dire de prévoir que les paramètres d'utilisation d'un service soient initialement réglés de manière à assurer la plus grande protection des renseignements personnels[77]. L'utilisateur devrait donc choisir de communiquer ses renseignements personnels de manière explicite. Selon M. Israel, de la CIPPIC, « le fait de reconnaître explicitement la protection des données personnelles par défaut mettrait d'autant plus en relief la nécessité d'obtenir l'approbation de l'utilisateur à l'égard des mécanismes de protection des renseignements personnels, ce qui contribuerait à réduire l'écart entre les attentes individuelles et la pratique[78] ». Cet avis est généralement partagé par Ian Kerr, professeur à l'Université d'Ottawa, qui indique que « tout réglage par défaut devrait être axé sur la protection des renseignements personnels[79] ».

David Fraser, associé chez McInnes Cooper, a cependant émis des réserves quant aux effets pratiques d'un système d'adhésion facultative par défaut. Lors de sa comparution, il a donné comme exemple la création d'un compte Twitter, une plateforme visant à faciliter l'expression publique. Comme il l'indique, si les réglages par défaut d'un compte Twitter favorisaient le plus haut niveau de protection « [c]ela aurait signifié qu'au jour un, lorsque vous vous seriez inscrits à Twitter, tous vos gazouillis auraient été protégés. Les premiers utilisateurs auraient crié dans une pièce vide[80] ».

Pour sa part, Paige Backman, associée chez Aird and Berlis LLP, recommande d'établir une distinction entre le traitement des renseignements personnels à des fins primaires – c'est-à-dire afin d'offrir le service auquel l'utilisateur a souscrit – et à des fins

---

76 *Ibid.*, p. 23.

77 Voir par ex. ETHI, *Témoignages*, 1re session, 42e législature, 21 mars 2017, 1615 (Michael Geist, titulaire de la chaire de recherche du Canada en droit d'Internet et du commerce électronique, professeur de droit, Université d'Ottawa, à titre personnel); ETHI, *Témoignages*, 1re session, 42e législature, 16 février 2017, 1640 (Vincent Gogolek).

78 ETHI, *Témoignages*, 1re session, 42e législature, 23 mars 2017, 1630 (Tamir Israel).

79 ETHI, *Témoignages*, 1re session, 42e législature, 4 avril 2017, 1720 (Ian Kerr, professeur et titulaire de la Chaire de recherche du Canada en éthique, en droit et en technologie, Université d'Ottawa, à titre personnel).

80 ETHI, *Témoignages*, 1re session, 42e législature, 21 mars 2017, 1630 (David Fraser, associé, McInnes Cooper, à titre personnel).

secondaires – par exemple le transfert à des tiers aux fins de marketing. Selon M[me] Backman, « une option quant au droit de renonciation pour de telles fins secondaires devrait être clairement énoncée et facilement accessible aux personnes qui lisent le document[81] ». La mise en place d'une telle pratique permettrait de renforcer le modèle du consentement en réduisant la prépondérance des « "acceptations" de tout ou rien ». M. Fraser établit une distinction similaire :

> Si je commande un livre chez Chapters-Indigo, dois-je donner mon consentement actif pour autoriser l'entreprise à utiliser l'adresse que je viens de lui fournir afin de m'envoyer le livre? La réponse est tout à fait évidente dans cette transaction, et ce consentement devrait être implicite. En revanche, une utilisation secondaire comme l'emploi de mon nom et de mon adresse aux fins de marketing, entre autres, semble être un élément sensible qui nécessite un consentement actif[82].

Le Comité est d'avis que l'adhésion facultative par défaut constitue un mécanisme prometteur afin de renforcer le modèle du consentement, bien qu'il puisse s'avérer nécessaire de le moduler afin de tenir compte du service offert. Au minimum, le Comité est d'avis que tout consentement visant l'utilisation des renseignements personnels à des fins secondaires devrait, par défaut, nécessiter un consentement.

Par conséquent, le Comité recommande :

Recommandation 2 sur l'adhésion facultative par défaut :

Que le gouvernement du Canada propose des modifications à la *Loi sur la protection des renseignements personnels et les documents électroniques* afin de prévoir explicitement l'adhésion facultative par défaut en ce qui a trait à toute utilisation des renseignements personnels à des fins secondaires, et la mise en place d'un système d'adhésion facultative par défaut sans égard à l'objectif poursuivi.

3. Améliorer la transparence algorithmique

Afin d'obtenir un consentement valable, il est essentiel que les individus disposent de suffisamment d'information sur la manière dont l'information est utilisée par les organisations qui la collectent, surtout à l'ère des mégadonnées et des transferts transfrontaliers[83]. De nos jours, les renseignements personnels sont souvent traités par des algorithmes complexes, qui peuvent viser à augmenter la qualité de l'expérience de l'utilisateur, mais parfois aussi à évaluer des risques et prendre des décisions

81 ETHI, Mémoire de Paige Backman et Aaron Baer, avril 2017.

82 ETHI, *Témoignages*, 1re session, 42e législature, 21 mars 2017, 1710 (David Fraser).

83 ETHI, *Témoignages*, 1re session, 42e législature, 21 mars 2017, 1620 (Michael Geist).

importantes pouvant affecter les intérêts des utilisateurs[84]. Or, « [l]a manière dont sont conçus ces programmes d'intelligence artificielle soulève des problèmes uniques en matière de protection des renseignements personnels[85] ». En effet, les utilisateurs disposent de peu d'information sur leur fonctionnement, sur les données qu'ils collectent et la manière dont elles sont utilisées.

L'une des craintes formulées à l'endroit des algorithmes a trait au risque que ces derniers fassent usage de renseignements personnels d'une manière qui perpétue des préjugés ou des pratiques discriminatoires qui existent dans notre société. À ce sujet, Valerie Steeves, professeure titulaire au département de criminologie à l'Université d'Ottawa, a notamment fait part au Comité d'un exemple relatif à un système de renseignement censé identifier de jeunes criminels en Angleterre. Selon M[me] Steeves, « [l]e plus jeune criminel potentiel identifié était âgé de trois ans, et il a été identifié parce qu'il était d'une certaine race et pauvre et qu'il vivait dans une région précise[86] ».

En plus des risques causés par des pratiques potentiellement discriminatoires, M. Kerr a fait valoir que l'utilisation des renseignements personnels par des algorithmes, en plus de leur grande opacité, peut nuire aux droits des individus :

> L'apprentissage automatique, la découverte de connaissances dans les banques de données et d'autres techniques relatives à l'intelligence artificielle produisent des modèles décisionnels qui sont si radicalement différents de la manière dont les décisions sont prises par des humains que nous n'arrivons pas à les comprendre. Fait ironique, l'intelligence artificielle fait preuve d'une précision incroyable, mais ceux qui s'en servent et même leurs programmeurs ne savent souvent pas exactement comment et pourquoi.
>
> Si nous permettons de telles décisions sans être en mesure de les comprendre, cela peut avoir l'effet d'éliminer les obstacles essentiels à la primauté du droit. Lorsqu'une institution utilise vos renseignements personnels et des données à votre sujet pour décider que votre prêt vous est refusé, que votre quartier fait l'objet d'une plus grande surveillance policière, que vous n'êtes pas admis à l'université, que vous n'obtenez pas l'emploi et que vous ne pouvez pas être remis en liberté et que personne ne peut vraiment expliquer ces décisions, de telles utilisations de vos données nuisent à vos droits relatifs à la protection des renseignements personnels[87].

84 ETHI, *Témoignages*, 1re session, 42e législature, 4 avril 2017, 1720 (Ian Kerr).

85 *Ibid.*

86 ETHI, *Témoignages*, 1re session, 42e législature, 16 février 2017, 1635 (Valerie Steeves, professeur titulaire, Département de criminologie, Université d'Ottawa, à titre personnel).

87 ETHI, *Témoignages*, 1re session, 42e législature, 4 avril 2017, 1635 (Ian Kerr).

En réponse à ces préoccupations, certains spécialistes souhaitent la mise en place de pratiques visant à favoriser une plus grande transparence de la part des organisations qui développent des algorithmes et qui en font usage. Michael Geist croit qu'il faut exiger que « les moteurs de recherche et les entreprises de médias sociaux divulguent la façon dont l'information est utilisée pour déterminer le contenu affiché à chaque utilisateur[88] ». M[me] Steeves abonde dans le même sens, faisant par ailleurs valoir que le régime législatif actuel prévoie déjà des exigences en matière de transparence qui sont applicables aux algorithmes :

> À bien des égards, c'est déjà dans nos lois […] C'est seulement que très souvent, c'est enterré dans l'algorithme d'une manière qui rend cela même moins transparent, et un certain nombre d'entre nous, dans le secteur de la société civile, sont très préoccupés par cela et pensent qu'il serait bon d'avoir une disposition distincte.
>
> Cela requiert en grande partie également que les entreprises soient plus responsables des résultats. Oui, je crois que des sanctions devraient être imposées lorsqu'il y a des résultats discriminatoires en particulier, et je pense que cela créerait une situation où les gens seraient beaucoup plus prudents lorsqu'ils utilisent des algorithmes qui changent de façon très importante les résultats concernant la vie des gens[89].

Le Comité croit que le consentement éclairé passe aussi par la mise en place de mesures visant à améliorer la transparence algorithmique. Qu'il s'agisse de modifications à la LPRPDE ou de la prise d'autres mesures, le Comité souhaite une plus grande transparence de la part des entreprises qui utilisent des algorithmes afin de traiter les renseignements personnels des Canadiennes et des Canadiens.

Par conséquent, le Comité recommande :

Recommandation 3 sur la transparence algorithmique :

Que le gouvernement du Canada envisage la prise de mesures visant à améliorer la transparence algorithmique.

4. La révocation du consentement

Un élément clé d'un consentement valable et éclairé à la collecte, l'utilisation et la communication de renseignements personnels est la capacité pour les individus de révoquer leur consentement de manière effective[90]. La LPRPDE prévoit qu'une personne

88 ETHI, *Témoignages*, 1re session, 42e législature, 21 mars 2017, 1620 (Michael Geist).

89 ETHI, *Témoignages*, 1re session, 42e législature, 16 février 2017, 1715 (Valerie Steeves); LPRPDE, annexe, art. 4.8 et 4.9.

90 ETHI, *Témoignages*, 1re session, 42e législature, 30 mai 2017, 1705 (Adam Kardash).

peut retirer son consentement en tout temps, sous réserve de restrictions législatives ou contractuelles applicables et d'un avis raisonnable[91]. Or, bien souvent, il existe « une multitude de situations actuelles dans lesquelles il est très difficile d'assurer en pratique le caractère révocable du consentement[92] ». Un bon exemple de ces difficultés a trait au retrait d'information personnelle des réseaux sociaux :

> Je crois que dans le cas où une personne avait affiché quelque chose la concernant et qu'elle voulait que ce soit supprimé, s'il n'y avait aucune autre raison contractuelle ou légale valide pour laquelle une organisation devrait conserver ou laisser cette information affichée, dans bien des cas, la LPRPDE exigerait aujourd'hui que cette information soit supprimée.
>
> Je crois que bon nombre de réseaux sociaux fonctionnent en effet de cette manière, aujourd'hui. Si vous affichez quelque chose dans plusieurs réseaux sociaux, il vous est possible de le retirer après l'avoir affiché. Cela ne change rien au fait que des gens ont vu cette information et, parfois, cela ne change rien au fait que d'autres personnes l'ont copiée et distribuée par d'autres moyens, mais il vous est possible de la retirer du réseau sur lequel vous l'aviez affichée[93].

Bref, les organisations ayant collecté, utilisé ou communiqué des renseignements personnels donnent généralement effet à la révocation du consentement en supprimant ces informations. Dans le contexte d'interactions simples entre les individus et ces organisations, il est possible de donner effet à une révocation de manière à complètement supprimer les renseignements personnels concernés. Or, dans le cadre d'interactions multiples – comme dans le cas des médias sociaux – il n'est pas nécessairement possible pour l'organisation de donner un effet complet à la révocation du consentement, car il se peut que les renseignements personnels de l'individu aient été copiés et retransmis par d'autres.

Le Comité est conscient du rôle clé que joue la révocation du consentement dans la capacité de maintenir un modèle viable de protection des renseignements personnels fondé sur le consentement. Le Comité reconnaît aussi les difficultés inhérentes à la mise en œuvre d'une telle révocation, difficultés qui sont étroitement liées à un autre enjeu traité dans ce rapport, soit la protection de la vie privée et de la réputation en ligne. Le gouvernement doit étudier ce sujet afin de mettre en place des mécanismes permettant de clarifier la manière dont le consentement peut être révoqué, ainsi que les conséquences pratiques et juridiques de ce geste.

---

91 LPRPDE, annexe, art. 4.3.8.

92 ETHI, *Témoignages*, 1re session, 42e législature, 30 mai 2017, 1705 (Adam Kardash).

93 ETHI, *Témoignages*, 1re session, 42e législature, 11 mai 2017, 1615 (David Elder, conseiller juridique spécial, Protection des renseignements personnels numériques, Association canadienne du marketing).

Par conséquent, le Comité recommande :

Recommandation 4 sur la révocation du consentement :

Que le gouvernement du Canada étudie la question de la révocation du consentement afin de clarifier la forme qu'elle doit prendre ainsi que ses effets juridiques et pratiques.

D. Exceptions à la règle générale du consentement

Au cours de son étude, le Comité a reçu de nombreux témoignages traitant d'exemptions – existantes et suggérées – à la règle générale du consentement. La présente section traite de certaines exemptions ayant attiré l'attention du Comité.

1. Les « renseignements auxquels le public a accès »

En vertu de la LPRPDE, il n'est pas nécessaire d'obtenir le consentement d'un individu afin de collecter, d'utiliser ou de communiquer un renseignement le concernant s'il s'agit d'un renseignement réglementaire auquel le public a accès[94]. Le *Règlement précisant les renseignements auxquels le public a accès*, entré en vigueur en 2001, détaille les types de renseignements, de même que leurs supports, qui sont ainsi exemptés de l'obligation d'obtenir un consentement. Voici les renseignements personnels exemptés prévus au règlement :

> a) les renseignements personnels — nom, adresse et numéro de téléphone des abonnés — figurant dans un annuaire téléphonique accessible au public, si l'abonné peut refuser que ces renseignements y figurent;
>
> b) les renseignements personnels, y compris les nom, titre, adresse et numéro de téléphone, qui figurent dans un répertoire, listage ou avis à caractère professionnel ou d'affaires qui est accessible au public, si la collecte, l'utilisation et la communication de ces renseignements sont directement liées à la raison pour laquelle ils figurent dans le répertoire, listage ou avis;
>
> c) les renseignements personnels qui figurent dans un registre, qui sont recueillis aux termes d'une autorisation législative et pour lesquels un droit d'accès public est autorisé par la loi, si la collecte, l'utilisation et la communication de ces renseignements sont directement liées à la raison pour laquelle ils figurent dans le registre;
>
> d) les renseignements personnels qui figurent dans un dossier ou document d'un organisme judiciaire ou quasi judiciaire, qui est accessible au public, si

94 LPRPDE, al. 7(1)*d*), (2)*c*.1) et (3)*h*.1).

> la collecte, l'utilisation et la communication de ces renseignements sont directement liées à la raison pour laquelle ils figurent dans le dossier ou document;
>
> e) les renseignements personnels qui figurent dans une publication, y compris les magazines, livres et journaux, sous forme imprimée ou électronique, qui est accessible au public, si l'intéressé a fourni les renseignements[95].

Cette définition est considérée comme désuète par plusieurs témoins. Elle a été qualifiée d'obsolète par Linda Routledge, directrice, Consommation à l'Association des banquiers canadiens, car « [l]e règlement actuel fait référence aux technologies dominantes au début des années 2000[96] ». Anny Duval, conseillère juridique à l'Association canadienne des compagnies d'assurances de personnes (ACCAP) note que « [l]a définition qui figure actuellement dans le Règlement précisant les renseignements auxquels le public a accès ne semble plus refléter la réalité ni les attentes des particuliers qu'elle vise à protéger[97] ». M[me] Duval propose d'élargir cette définition afin qu'elle couvre l'ensemble des situations dans lesquelles un individu affiche des renseignements personnels sur un site Internet accessible au public[98]. M. Watson, de l'ACTI, propose quant à lui de modifier la définition de manière à la rendre neutre sur le plan technologique, à l'instar de la LPRPDE, ce qui lui permettrait de mieux s'adapter aux évolutions technologiques[99].

Le CPVP est aussi d'avis que le règlement devrait être mis à jour. Cependant, ce dernier émet une réserve :

> Toutefois, nous faisons une mise en garde contre la fausse idée souvent véhiculée que les renseignements personnels ne présentent aucun intérêt sur le plan de la protection de la vie privée simplement parce qu'ils sont généralement accessibles en ligne.
>
> La décision concernant la façon de protéger la vie privée des individus dont les renseignements sont accessibles au public est extrêmement complexe […] Au bout du compte, vu l'importance de cet enjeu, une simple modification du règlement par le gouverneur en conseil ne serait cependant pas suffisante. Le sujet mérite plutôt que le

---

95 *Règlement précisant les renseignements auxquels le public a accès*, DORS/2001-7.

96 ETHI, *Témoignages*, 1re session, 42e législature, 11 mai 2017, 1540 (Linda Routledge, directrice, Consommation, Association des banquiers canadiens).

97 ETHI, *Témoignages*, 1re session, 42e législature, 30 mai 2017, 1535 (Anny Duval, conseillère juridique, Association canadienne des compagnies d'assurances de personnes).

98 *Ibid.*

99 ETHI, *Témoignages*, 1re session, 42e législature, 16 mai 2017, 1550 (Robert Watson); ETHI, *Témoignages*, 1re session, 42e législature, 30 mai 2017, 1610 (Adam Kardash).

> Parlement l'étudie attentivement et en débatte, car ces questions doivent faire l'objet d'une réflexion approfondie; il faut pouvoir trouver un équilibre entre les droits fondamentaux [de] l'individu et ceux de la société[100].

Le Comité convient que la définition réglementaire des renseignements auxquels le public a accès est désuète et doit être mise à jour. Qui plus est, le Comité croit que, à l'instar de la LPRPDE, le règlement devrait être neutre sur le plan technologique.

Par conséquent, le Comité recommande :

Recommandation 5 sur le *Règlement précisant les renseignements auxquels le public a accès* :

Que le gouvernement du Canada modernise le *Règlement précisant les renseignements auxquels le public a accès* afin de tenir compte des situations dans lesquelles un individu affiche des renseignements personnels sur un site Internet accessible au public et afin de rendre le *Règlement* neutre sur le plan technologique.

2. Les intérêts d'affaires légitimes

Plusieurs témoins entendus par le Comité ont traité des modalités de l'utilisation de renseignements personnels afin de satisfaire les intérêts d'affaires légitimes des entreprises. À l'heure actuelle, et sous réserve d'exceptions limitées, la LPRPDE prévoit qu'une organisation ne peut exiger un consentement relativement à la collecte, l'utilisation ou la communication de renseignements personnels « autres que ceux qui sont nécessaires pour réaliser les fins légitimes et explicitement indiquées[101] » et qu'elle peut le faire uniquement « à des fins qu'une personne raisonnable estimerait acceptables dans les circonstances[102] ». Or, comme l'indique le CPVP, le consentement explicite est souvent difficile à demander et à obtenir dans certaines situations, par exemple lors de l'utilisation d'un moteur de recherche, dans le contexte du traitement des mégadonnées, ou bien lorsque de nouvelles possibilités d'utilisation apparaissent après la collecte initiale[103].

Face à cette situation, quelques témoins ont revendiqué une nouvelle exemption à la règle du consentement applicable aux intérêts d'affaires légitimes. Il s'agit d'une exemption inspirée du modèle européen, qui permet l'utilisation de renseignements

---

100 CPVP, *Rapport annuel au Parlement 2016-2017*, septembre 2017, p. 32.

101 LPRPDE, annexe 1, art. 4.3.3.

102 LPRPDE, art. 5(3).

103 CPVP, *Rapport annuel au Parlement 2016-2017*, septembre 2017, p. 17-18.

personnels sans consentement lorsque le traitement de ces données est nécessaire pour les fins légitimes poursuivies par les organisations[104]. M[me] Routledge, de l'Association des banquiers canadiens, décrit ainsi l'exemption proposée :

> Nous suggérons, comme moyen possible de répondre à cette préoccupation, de simplifier les avis de confidentialité afin de rendre le consentement non requis pour les usages auxquels les personnes s'attendent et qu'elles considèrent comme raisonnables. Plus particulièrement, nous soutenons qu'un consentement explicite ne devrait pas être requis dans le cas des fins commerciales légitimes, dont voici certains exemples. Les fins pour lesquelles les renseignements personnels ont été recueillis, la prestation de services, la compréhension ou la livraison de produits ou de services qui répondent aux besoins des clients et la formation dans le cadre du service à la clientèle.[105]

Selon M[me] Routledge, une telle exemption à la règle du consentement aurait des effets bénéfiques pour les consommateurs dans la mesure où les avis de confidentialité s'en trouveraient grandement simplifiés, ce qui faciliterait un meilleur consentement éclairé[106]. Selon elle, les consommateurs pourraient « se concentrer sur les renseignements d'importance pour eux et à l'égard desquels ils peuvent agir[107] ».

Cependant, le CPVP est d'avis qu'une telle exception n'est pas souhaitable. Dans son rapport annuel 2016–2017, le CPVP a soulevé deux motifs à l'encontre d'une exception générale liée à « l'intérêt légitime ». D'une part, il considère ce concept comme trop large, englobant des situations dans lesquelles « une exception en matière de consentement n'est pas nécessaire[108] ». D'autre part, en raison de l'élasticité potentielle des « intérêts légitimes » des entreprises, le risque d'abus est trop important[109]. Le CPVP indique toutefois que plusieurs membres de l'industrie ayant participé à son étude sur le consentement ont indiqué qu'il pourrait être indiqué d'appliquer le concept de consentement implicite à ces situations[110]. Le CPVP indique aussi qu'il existe « des arguments en faveur d'une description des fins visées (comme "améliorer le service à la

104 ETHI, *Témoignages*, 1re session, 42e législature, 30 mai 2017, 1535 (Frank Zinatelli); ETHI, *Témoignages*, 1re session, 42e législature, 30 mai 2017, 1600 (Adam Kardash).

105 ETHI, *Témoignages*, 1re session, 42e législature, 11 mai 2017, 1540 (Linda Routledge).

106 *Ibid.*

107 *Ibid.*

108 CPVP, *Rapport annuel au Parlement 2016-2017*, septembre 2017, p. 34.

109 *Ibid.*

110 *Ibid.*, p. 18; ETHI, Mémoire de l'Association canadienne de Marketing, mai 2017.

clientèle") qui autoriserait les organisations à utiliser les renseignements à des fins non connues au moment de la collecte[111] ».

Le Comité est d'avis que des mesures doivent être prises afin de répondre aux préoccupations existantes quant aux utilisations acceptables pour des intérêts d'affaires légitimes. Toutefois, le Comité partage les préoccupations exprimées par plusieurs témoins quant à la mise en place d'une nouvelle exemption à la règle du consentement applicable aux intérêts d'affaires légitimes.

Par conséquent, le Comité recommande :

Recommandation 6 sur les intérêts d'affaires légitimes :

Que le gouvernement du Canada envisage de modifier la *Loi sur la protection des renseignements personnels et les documents électroniques* afin de clarifier les modalités de l'utilisation de renseignements personnels afin de satisfaire les intérêts d'affaires légitimes des entreprises.

3. La dépersonnalisation

Le Comité s'est également penché sur la collecte, l'utilisation et la communication de données dépersonnalisées (aussi appelées « anonymisées » ou « désidentifiées »), c'est-à-dire les données agrégées et présentées de sorte qu'il soit impossible d'identifier à qui elles appartiennent. Selon le CPVP, la dépersonnalisation présente à la fois des avantages et des inconvénients pour la protection de la vie privée :

> D'une part, on peut y recourir pour trouver un équilibre entre la protection des renseignements personnels et le souhait des organisations d'utiliser ces renseignements de façons nouvelles et novatrices. D'autre part, on s'inquiète du fait qu'il puisse tout simplement être impossible de désidentifier complètement les renseignements personnels sans qu'il reste un risque de réidentification[112].

Il existe un certain débat à savoir si les données dépersonnalisées devraient être considérées comme des renseignements personnels aux fins de la LPRPDE. M^e^ Bernier est d'avis que, à l'instar de ce qui est prévu en droit européen, on devrait préciser que « l'anonymisation constitue une façon de soustraire les renseignements personnels à

111 CPVP, *Rapport annuel au Parlement 2016-2017*, septembre 2017, p. 18.

112 CPVP, *Rapport annuel au Parlement 2016-2017*, septembre 2017, p. 31; au sujet du risque de réidentification, voir aussi ETHI, *Témoignages*, 1re session, 42e législature, 21 février 2017, 1530 (Drew McArthur, commissaire par intérim, Bureau du Commissaire à l'information et à la protection de la vie privée de la Colombie-Britannique).

l'application de la loi[113] ». D'autres croient plutôt que, bien qu'assujetties à la *Loi*, ces données devraient être soustraites à l'exigence du consentement[114].

Dans son rapport annuel 2016–2017, le CPVP a noté la complexité de cette question et a fait part de son intention de publier un document d'information au sujet de la dépersonnalisation des données[115]. De plus, il encourage le Parlement « à examiner cette nouvelle question, qui pourrait assurer la souplesse nécessaire pour atteindre un meilleur équilibre entre la protection de la vie privée et la valeur économique des données[116] ». Cela étant, il croit que la dépersonnalisation « pourrait être une solution viable pourvu qu'elle soit gérée correctement[117] ».

Le Comité est conscient de l'importance de protéger les données dépersonnalisées et de mettre des mesures en place afin de réduire au minimum le risque que des données soient réidentifiées. Bien que la création d'une exception à la règle du consentement relative aux données dépersonnalisées constitue une avenue possible, le Comité considère qu'il serait prématuré d'en faire la recommandation à l'heure actuelle.

Par conséquent, le Comité recommande :

Recommandation 7 sur les données dépersonnalisées :

Que le gouvernement du Canada étudie les meilleurs moyens de protéger les données dépersonnalisées.

4. Les crimes financiers

Depuis l'entrée en vigueur d'une modification à la LPRPDE de 2015, il est permis à des organisations, dans certaines circonstances, de communiquer des renseignements personnels à une autre organisation, sans le consentement de l'individu, dans des cas liés à des enquêtes ou à des fraudes[118]. Lors de l'étude du Comité, M^me^ Routledge, de l'Association des banquiers canadiens, a fait valoir que la « fraude » n'est pas la seule activité économique criminelle à laquelle les institutions financières font face et pour

113 ETHI, *Témoignages*, 1re session, 42e législature, 14 février 2017, 1545 (Chantal Bernier).

114 Voir notamment ETHI, *Témoignages*, 1re session, 42e législature, 30 mai 2017, 1550 (Randy Bundus, vice-président principal, conseiller juridique en chef, Bureau d'assurance du Canada); ETHI, *Témoignages*, 1re session, 42e législature, 30 mai 2017, 1600 (Adam Kardash).

115 CPVP, *Rapport annuel au Parlement 2016-2017*, septembre 2017, p. 31.

116 *Ibid.*, p. 32.

117 *Ibid.*, p. 31.

118 LPRPDE, al. 7(3)*d*.2).

laquelle la transmission d'informations est importante. Elle note que cette « définition ne s'étend pas à d'autres types d'activité criminelle comme le vol de données ou de renseignements personnels, le blanchiment d'argent, le financement d'activités terroristes, les crimes cybernétiques et même les vols de banque[119] ».

Afin de remédier à cette lacune dans la LPRPDE, M^me^ Routledge recommande le remplacement de l'expression « fraude » par celle de « crimes financiers » et que ce terme soit défini dans la *Loi* de manière à inclure :

> premièrement, la fraude, deuxièmement, les activités criminelles et toute infraction sous-jacente liée au blanchiment d'argent et au financement d'activités terroristes, troisièmement, d'autres infractions criminelles perpétrées contre des institutions financières, leurs clients et leurs employés, et, quatrièmement, le manquement aux lois de pays étrangers, notamment en ce qui concerne le blanchiment d'argent et le financement d'activités terroristes[120].

Un tel changement, de l'avis de M^me^ Routledge, permettrait d'améliorer la capacité des banques de lutter contre les crimes financiers[121]. Le Comité est d'accord et par conséquent recommande :

Recommandation 8 sur les crimes financiers :

a) Que l'alinéa 7(3)d.2) de la *Loi sur la protection des renseignements personnels et les documents électroniques* soit modifié de manière à remplacer l'expression « fraude » par celle de « crime financier ».

b) Qu'un « crime financier » soit défini dans la *Loi* de manière à y inclure :

- **la fraude;**
- **les activités criminelles et toute infraction sous-jacente liée au blanchiment d'argent et au financement d'activités terroristes;**
- **toutes infractions criminelles perpétrées contre des fournisseurs de services financiers, leurs clients ou leurs employés;**
- **le manquement aux lois de pays étrangers, notamment en ce qui concerne le blanchiment d'argent et le financement d'activités terroristes.**

119 ETHI, *Témoignages*, 1re session, 42e législature, 11 mai 2017, 1545 (Linda Routledge).

120 *Ibid.*

121 *Ibid.*

E. Le consentement et la protection des mineurs

L'application aux personnes mineures du modèle de protection des renseignements personnels fondé sur le consentement soulève des enjeux particuliers. En effet, plusieurs témoins ont fait part de leurs préoccupations quant à la connaissance qu'ont les jeunes des enjeux relatifs à la protection des renseignements personnels, de même que leur capacité de consentir à la collecte, l'utilisation et la transmission de ces renseignements.

Lors d'une étude conduite à l'automne 2016, M[me] Steeves a constaté qu'aucun des jeunes âgés entre 13 et 16 ans qu'elle a rencontrés ne connaissait des pratiques équitables en matière de renseignements ni se souvenait de son consentement à la collecte de ses renseignements lors de son inscription sur divers réseaux sociaux ou lors de la publication de matériel sur ces réseaux[122]. Elle indique que ces jeunes considèrent que les politiques de confidentialité « ont été délibérément rédigées pour les vexer et les embrouiller, afin de les empêcher de comprendre ce qui se passe et faire en sorte qu'ils se sentent impuissants[123] ». M[me] Steeves a également fait valoir au Comité qu'il existe une grande disparité entre les attentes des jeunes et la réalité :

> En 2015, nous avons mené un sondage auprès de 5 500 jeunes de 10 à 17 ans de partout au pays. Nous leur avons demandé qui devrait être en mesure de voir ce qu'ils publient en ligne, et 83 % d'entre eux ont répondu que les entreprises propriétaires des plateformes sur lesquelles ils publient des renseignements ne devraient pas avoir accès à ces renseignements […] Et 95 % d'entre eux ont affirmé que les spécialistes en marketing ne devraient pas être en mesure de voir leurs publications […]
>
> Je crois que cet aperçu laisse fortement penser qu'il y a un manque de cohérence entre le modèle de réglementation et les expériences vécues par les gens qui se divertissent, magasinent, étudient et passent du temps sur ces plateformes[124].

Il existe aussi des préoccupations quant au moment auquel un adolescent est suffisamment mature pour être en mesure de donner son consentement à la collecte, à l'utilisation ou à la communication de ses renseignements personnels[125].

En réponse à ces préoccupations, plusieurs témoins ont proposé la mise en place d'un âge minimal nécessaire pour qu'un individu puisse donner un consentement valable en matière de divulgation de renseignements personnels. Quelques témoins ont suggéré

---

122 ETHI, *Témoignages*, 1re session, 42e législature, 16 février 2017, 1630 (Valerie Steeves).

123 *Ibid.*

124 *Ibid.*

125 ETHI, *Témoignages*, 1re session, 42e législature, 14 février 2017, 1655 (John Lawford).

un âge minimal fixé à 16 ans[126]. Cet âge est généralement conforme aux règles européennes et, pour les plus jeunes, le consentement devrait être obtenu des parents et il faudrait être en mesure de vérifier qu'un parent a bel et bien consenti :

> Toute méthode utilisée pour obtenir le consentement vérifiable devrait être calculée de façon raisonnable, en tenant compte de la nouvelle technologie, pour s'assurer que la personne qui donne son consentement est bel et bien le parent de l'enfant ou le tuteur légal. Bien que l'âge fixé à 16 ans ne soit pas un chiffre magique, il respecte les lois nationales et internationales, notamment le Règlement général sur la protection des données, le RGPD. Au sujet de l'approche utilisée pour obtenir le consentement du parent ou du tuteur, nos recommandations sont conformes au règlement sur la protection des enfants sur Internet de la FTC américaine ainsi qu'au RGPD dont l'exigence imposée aux organisations consiste à déployer des efforts raisonnables pour obtenir le consentement vérifiable d'un parent en tenant compte des technologies existantes[127].

Owen Charters, président-directeur général de Repaires jeunesse du Canda (RJC), propose d'interdire la collecte, l'utilisation et la divulgation des renseignements personnels des enfants de moins de 13 ans. À son avis, ces derniers sont tout simplement « trop jeunes pour comprendre les conséquences de la collecte et de l'utilisation des données[128] ». M. Charters a également noté que les États-Unis disposent d'une loi qui traite spécifiquement de la protection de la vie privée des mineurs. Cette loi, la *Children's Online Privacy Protection Act*, exige le consentement parental pour recueillir les renseignements personnels des enfants de moins de 13 ans. De plus, en Europe, le RGPD exige le consentement d'un parent ou d'un tuteur pour accéder à des services en ligne pour les enfants de moins de 16 ans, ou moins, pourvu que l'âge prévu soit d'au moins 13 ans[129]. Selon Dennis Hogarth, du Conseil des consommateurs du Canada, « [t]ant qu'il n'existe pas une sorte de système de registre fiable pour vérifier l'âge, il sera difficile de procéder à des contrôles sans créer de nouveaux problèmes de protection de la vie privée[130] ».

---

126 Voir par ex. *Ibid.*; ETHI, *Témoignages*, 1re session, 42e législature, 16 mai 2017, 1555 (Dennis Hogarth, vice-président, Conseil des consommateurs du Canada); ETHI, *Témoignages*, 1re session, 42e législature, 6 avril 2017, 1635 (Paige Backman, associée, Aird and Berlis LLP, à titre personnel); ETHI, *Témoignages*, 1re session, 42e législature, 25 septembre 2017, 1535 (Owen Charters, président-directeur général, Repaires jeunesse du Canada).

127 ETHI, *Témoignages*, 1re session, 42e législature, 6 avril 2017, 1635 (Paige Backman).

128 ETHI, *Témoignages*, 1re session, 42e législature, 25 septembre 2017, 1535 (Owen Charters).

129 *Ibid.*, 1655.

130 ETHI, *Témoignages*, 1re session, 42e législature, 16 mai 2017, 1555 (Dennis Hogarth).

M. Karanicolas, du CLD, note toutefois qu'il demeure possible, à l'heure actuelle, de duper les systèmes de vérification de l'âge, ce qui donne un caractère quelque peu artificiel à l'imposition d'un âge minimal de consentement[131].

Enfin, l'ancienne commissaire Stoddart a émis certaines réserves quant à l'imposition de règles visant spécifiquement les mineurs puisque ces questions pourraient tomber dans le champ de compétence des provinces. Selon M[me] Stoddart, afin d'éviter des conflits de champs de compétence, il vaudrait mieux aborder la question des mineurs « sous l'angle du renforcement du principe du consentement » plutôt qu'en imposant un âge spécifique[132].

Étant donné la grande utilisation des technologies de l'information chez les jeunes et étant donné qu'ils forment un groupe particulièrement vulnérable sur le plan de la protection de la vie privée, le Comité est d'avis que des mesures spéciales devraient être mises en place afin de régir leur capacité d'offrir un consentement valable. Des mesures devraient également être mises en place afin de limiter la capacité des organisations de collecter, d'utiliser et de communiquer des renseignements personnels concernant des personnes mineures.

Par conséquent, le Comité recommande :

Recommandation 9 sur les règles de consentement spécifiques pour les mineurs :

Que le gouvernement du Canada envisage la mise en place de règles de consentement spécifiques pour les mineurs ainsi que la mise en place de règles concernant la collecte, l'utilisation et la communication de renseignements personnels concernant les mineurs.

F. La portabilité des données

Comme indiqué précédemment, le principe du consentement repose en grande partie sur la notion que les individus doivent demeurer aussi libres que possible de choisir la façon dont ils disposent de leurs renseignements personnels. Or, cette liberté de choisir ne devrait pas être restreinte à la capacité de consentir à la collecte, l'utilisation et la communication de leurs renseignements personnels ou de retirer ce consentement. Le Comité est d'avis qu'il est aussi important que les individus soient en mesure de transférer leurs renseignements personnels entre prestataires de services de manière à pouvoir les réutiliser.

131 ETHI, *Témoignages*, 1re session, 42e législature, 23 février 2017, 1635 (Michael Karanicolas).

132 ETHI, *Témoignages*, 1re session, 42e législature, 23 mars 2017, 1710 (Jennifer Stoddart, à titre personnel).

Ce droit à la « portabilité des données » est reconnu dans l'UE à l'article 20 du RGDP, qui prévoit plusieurs situations dans lesquelles :

> [l]es personnes concernées ont le droit de recevoir les données à caractère personnel les concernant qu'elles ont fournies à un responsable du traitement, dans un format structuré, couramment utilisé et lisible par machine, et ont le droit de transmettre ces données à un autre responsable du traitement sans que le responsable du traitement auquel les données à caractère personnel ont été communiquées y fasse obstacle[133].

Ainsi, le droit à la portabilité des données implique que les fournisseurs de services s'assurent que leurs méthodes de collecte et de stockage des renseignements personnels soient suffisamment compatibles avec les méthodes de leurs compétiteurs afin que les utilisateurs soient en mesure de demander et d'obtenir un transfert de leurs renseignements d'un fournisseur vers un autre.

Le Comité est d'avis qu'un tel droit devrait être reconnu explicitement dans la LPRPDE.

Par conséquent, le Comité recommande :

Recommandation 10 sur la portabilité des données :

Que le gouvernement du Canada modifie la *Loi sur la protection des renseignements personnels et les documents électroniques* afin d'y prévoir un droit à la portabilité des données.

PARTIE 3 : RÉPUTATION EN LIGNE ET RESPECT DE LA VIE PRIVÉE

La protection de la réputation en ligne et le respect de la vie privée sont des enjeux de taille en matière de protection des renseignements personnels. La permanence des renseignements publiés sur Internet entraîne des risques importants en matière de réputation et soulève des questions quant à la capacité du régime de la LPRPDE d'assurer le respect de la vie privée des Canadiens. Dans ce rapport, le Comité aborde deux enjeux ayant trait à la protection de la réputation en ligne et le respect de la vie privée. Premièrement, il abordera la question de la permanence des données et du « droit à l'oubli ». Deuxièmement, le Comité traitera du concept de protection de la vie privé dès la conception des produits et services nécessitant la collecte, l'utilisation et la communication de renseignements personnels.

Avant de poursuivre, il est utile de rappeler que, sur le plan de la protection de la réputation en ligne, le régime de la LPRPDE n'opère pas en vase clos. Comme l'a indiqué

133 Règlement général sur la protection des données, Reg 2016/679 (UE), art. 20.

M[e] Bernier, plusieurs lois fédérales et provinciales ont un rôle à jouer dans ce domaine[134]. Ainsi, les atteintes à la réputation qui ne surviennent pas dans le cadre de transactions commerciales, mais plutôt dans le cadre de relations personnelles ne relèvent pas de la LPRPDE. Elles vont généralement être couvertes par des lois provinciales régissant la responsabilité civile et délictuelle[135]. De plus, au niveau fédéral, le *Code criminel* prévoit plusieurs infractions applicables, dont l'article 162.1, qui criminalise la transmission non consensuelle d'images intimes[136]. Par conséquent, cette partie du rapport se concentrera surtout sur les questions de protection de la vie privée et de la réputation en ligne dans le contexte des relations commerciales.

A. Le droit à l'oubli

L'une des conséquences importantes de l'avènement des nouvelles technologies de l'information sur la protection de la réputation et le respect de la vie privée est la facilité de recherche et d'accès ainsi que la permanence des renseignements personnels se retrouvant sur Internet. Cette réalité peut avoir des effets importants sur la réputation en ligne, surtout dans le cas de renseignements concernant des mineurs. Comme l'explique le CPVP, « [e]n raison de la permanence de l'information en ligne, le temps n'efface plus les erreurs ou les mauvaises décisions du passé[137] ».

C'est à cette problématique que l'on doit l'apparition du concept de « droit à l'oubli », qui s'est surtout développée en Europe, et qui s'entend des mesures qui peuvent être prises afin d'éviter que certains renseignements potentiellement préjudiciables concernant la réputation d'un individu hantent ce dernier pour une période indéfinie. Bien qu'il s'agisse d'un terme populaire, l'expression « droit à l'oubli » est imprécise et renvoie généralement à l'une ou l'autre des deux notions suivantes :

- Le *droit à l'effacement*, c'est-à-dire le droit au retrait d'informations sur un site Internet;

- Le *droit au déréférencement* (que certains témoins ont appelé « désindexation » ou « délistage »), c'est-à-dire le droit au retrait de la

134 ETHI, *Témoignages*, 1re session, 42e législature, 14 février 2017, 1550 (Chantal Bernier).

135 ETHI, *Témoignages*, 1re session, 42e législature, 14 février 2017, 1550 (Chantal Bernier). Me Bernier note que la Colombie-Britannique, le Manitoba, la Saskatchewan et Terre-Neuve-et-Labrador ont adoptés des lois qui créent un droit de recours explicite en responsabilité civile pour une violation à la vie privée. Au Québec, il est possible de s'adresser à un juge pour obtenir des ordonnances visant à faire cesser une atteinte à la réputation en ligne.

136 *Code Criminel*, LRC 1985, ch. C-46, art. 162.1.

137 CPVP, Réputation en ligne. Que dit-on à mon sujet?, janvier 2016; ETHI, *Témoignages*, 1re session, 42e législature, 16 mai 2017, 1545 (Robert Watson).

page Web contenant l'information des résultats de recherche de moteurs de recherche comme Google.

1. Le droit à l'effacement des données

À l'heure actuelle, la LPRPDE comprend des dispositions très limitées en matière de suppression, de correction des renseignements personnels et d'exactitude des données.

En ce qui concerne les renseignements ayant été communiqués à un fournisseur de services par la personne elle-même, la LPRPDE prévoit la possibilité pour la personne de retirer son consentement et d'exiger la suppression des renseignements personnels, sauf dans certaines situations, par exemple en raison de la présence de dispositions contractuelles prévoyant le contraire[138]. Ainsi, lorsqu'une personne souhaite retirer l'information personnelle qu'elle a transmise sur un réseau social, par exemple, la personne possède un droit absolu de le faire[139]. La *Loi* prévoit aussi que l'on « devrait détruire, effacer ou dépersonnaliser les renseignements personnels dont on n'a plus besoin aux fins précisées[140] ».

La situation se complique lorsqu'il est question d'obtenir la suppression de renseignements personnels concernant un individu qui ont été transmis à un fournisseur de services par une autre personne. Il peut s'agir, par exemple, du partage sur les réseaux sociaux, d'une photo ou d'un message initialement publié par un tiers, ou d'une publication indépendante contenant des renseignements personnels. Dans ces situations, la LRPDE fournit très peu d'outils permettant à un individu d'obtenir la suppression de ces renseignements, publiés sans son consentement initial[141]. Le principe 4.9.5 de l'annexe de la LPRPDE prévoit que les organisations doivent corriger les renseignements incomplets, inexacts ou qui ne sont plus à jour et le paragraphe 5(3) prévoit qu'une organisation ne peut recueillir, utiliser ou communiquer des renseignements personnels qu'à des fins qu'une personne raisonnable estimerait acceptables dans les circonstances. Selon le CPVP, ces deux dispositions pourraient permettre d'obtenir l'effacement de certains renseignements personnels publiés par des tiers dans les circonstances limitées par ces deux dispositions[142]. Autrement, la LPRPDE ne prévoit pas de droit de l'intéressé d'obtenir la suppression de

138 LPRPDE, annexe, art. 4.3.8; CPVP, *Projet de position du Commissariat sur la réputation en ligne*, 26 janvier 2018.

139 ETHI, *Témoignages*, 1re session, 42e législature, 1er février 2018, 0930 (Daniel Therrien).

140 LPRPDE, annexe, art. 4.5.3; CPVP, *Projet de position du Commissariat sur la réputation en ligne*, 26 janvier 2018.

141 *Ibid.*

142 CPVP, *Projet de position du Commissariat sur la réputation en ligne*, 26 janvier 2018.

renseignements publiés par un tiers, qui est par ailleurs protégé par la liberté d'expression garantie à l'alinéa 2*b*) de la *Charte canadienne des droits et libertés*.

Le Comité note aussi qu'il existe au moins une décision judiciaire canadienne à l'issue de laquelle on a ordonné la suppression de données publiées sur Internet dans des circonstances allant à l'encontre de la LPRPDE. Il s'agit de la décision récente de la Cour fédérale dans l'affaire *A.T. c. Globe24h.com*[143]. Dans cette affaire, la Cour fédérale a ordonné le retrait d'un site Internet de nature commerciale hébergé en Roumanie de toute jurisprudence canadienne contenant des renseignements personnels, car leur présence sur ce site Internet ne constituait pas une utilisation acceptable au titre du paragraphe 5(3) de la LPRPDE[144]. Le Comité est toutefois conscient qu'il s'agit d'une décision isolée et note que le défendeur n'a pas participé à l'instance[145].

Malgré les quelques éléments qui existent à l'heure actuelle en matière d'effacement des renseignements personnels, force est de constater que la LPRPDE est loin de prévoir un régime exhaustif et ne permet pas de recours, par exemple, lorsque des renseignements personnels véridiques et potentiellement préjudiciables sont mis en ligne par des tiers[146]. Il pourrait s'agir, par exemple, de gestes et de photos embarrassants, mais aussi de certains actes de cyberintimidation et de pornographie de vengeance. Or, la présence de ces renseignements sur Internet peut avoir de lourdes conséquences pour les individus, surtout lorsqu'il s'agit de mineurs. M[me] Backman a soulevé cet enjeu lors de son témoignage :

> Les avantages pour les enfants et les jeunes de participer à des activités en ligne grâce aux médias sociaux sont nombreux. Cependant, une erreur de jugement d'un mineur, ou de jugement d'une autre personne qui vise l'information d'un mineur, peut avoir de lourdes conséquences à court et à long terme tant pour le mineur que la société. Nous constatons plus souvent une empreinte en ligne, provenant de la personne responsable, d'un mineur ou d'un enfant, ou de quelqu'un d'autre, ce qui peut largement contribuer au problème d'intimidation en ligne. Une telle intimidation peut bouleverser la santé physique et mentale de l'enfant et peut avoir des conséquences à long terme pour le mineur et la société[147].

---

143 *A.T. c. Globe24h.com*, 2017 CF 114.

144 Le paragraphe 5(3) de la LPRPDE prévoit qu'une organisation « ne peut recueillir, utiliser ou communiquer des renseignements personnes qu'à des fins qu'une personne raisonnable estimerait acceptables dans les circonstances ».

145 ETHI, *Témoignages*, 1re session, 42e législature, 21 mars 2017, 1625 (David Fraser).

146 ETHI, *Témoignages*, 1re session, 42e législature, 21 février 2017, 1530 (Drew McArthur).

147 ETHI, *Témoignages*, 1re session, 42e législature, 6 avril 2017, 1635 (Paige Backman).

Face à ces lacunes présentes dans la LPRPDE, plusieurs témoins ont recommandé la reconnaissance en droit canadien d'un droit à l'effacement similaire à celui reconnu dans l'UE par le biais du RGPD, qui entrera en vigueur en mai 2018[148]. Le RGPD confère aux individus le droit à l'effacement de leurs données personnelles, notamment :

- lorsque ces données ne sont plus nécessaires,
- lors de la révocation du consentement et qu'il n'existe pas de fondement juridique prévenant la suppression;
- dans les situations où l'individu s'oppose au traitement de ces données et qu'il n'existe aucun « motif légitime impérieux » justifiant qu'elles soient conservées;
- lorsque les données ont fait l'objet d'un traitement illicite[149].

Le RGPD prévoit toutefois certaines exceptions à ce droit, notamment afin de permettre aux organisations de se conformer à leurs obligations juridiques et afin de ne pas nuire à la liberté d'expression, la liberté de la presse et le droit à l'information[150].

Ceux qui favorisent l'adoption d'un droit à l'effacement dans la LPRPDE considèrent qu'il, s'agit, tout comme le renforcement du consentement, d'un moyen efficace de donner aux individus un plus grand contrôle sur leurs renseignements personnels. Comme l'indique Alysia Lau, conseillère juridique au Centre pour la défense de l'intérêt public (CDIP) : « Les Canadiens doivent avoir le choix et pouvoir exercer un contrôle sur la façon dont leurs données personnelles sont utilisées, y compris par le consentement, la rectification d'information et particulièrement la suppression ou l'effacement de renseignements les concernant[151]. » M^me^ Scassa abonde dans le même sens, considérant que l'effacement des données est un élément important lors de la fin d'une relation entre un individu et une entreprise du secteur privé, par exemple un site de réseautage[152]. De plus, Kristjan Backman, de l'Association nationale de destruction de

148 Règlement général sur la protection des données, Reg 2016/679 (UE).

149 *Ibid.*, art. 17(1); ETHI, *Témoignages*, 1re session, 42e législature, 14 février 2017, 1605 (Alysia Lau, conseillère juridique, Centre pour la défense de l'intérêt public).

150 Règlement général sur la protection des données, Reg 2016/679 (UE), art. 17(3); ETHI, *Témoignages*, 1re session, 42e législature, 23 février 2017, 1615 (Florian Martin-Bariteau, professeur adjoint, Section de common law, Faculté de droit, et directeur, Centre de recherche en droit, technologie et société, Université d'Ottawa, à titre personnel).

151 ETHI, *Témoignages*, 1re session, 42e législature, 14 février 2017, 1605 (Alysia Lau).

152 ETHI, *Témoignages*, 1re session, 42e législature, 23 février 2017, 1610 (Teresa Scassa) et 1615 (Florian Martin-Bariteau).

l'information – Canada (ANDI), affirme qu'un cadre législatif clair concernant la destruction de l'information lorsqu'elle n'est plus nécessaire constitue un moyen efficace de « garantir que les renseignements à caractère privé et professionnel ne soient pas exploités à d'autres fins que ceux établis initialement[153] ».

Le droit à l'effacement est aussi considéré comme important afin d'éviter que des erreurs de jugement commises par des mineurs – par exemple l'affichage de photos inappropriées sur Internet – aient de lourdes conséquences à court et à long terme. Cette préoccupation fut notamment soulevée par M. Charters, de RJC, qui appuie un droit à l'effacement applicable aux mineurs lors de l'atteinte de l'âge de la majorité :

> Les choix [que les enfants] font lorsqu'ils sont mineurs ne reflètent pas nécessairement l'identité et les préférences qu'ils afficheront quand ils auront atteint la majorité. Nous savons qu'il y a également bien des gens qui aimeraient que leur vie en ligne soit effaçable et oubliée et nous pensons que les enfants devraient effectivement pouvoir bénéficier de ce droit[154].

M[me] Backman, qui a pris position en faveur de la reconnaissance d'un droit d'effacement limité dans le cas des mineurs est aussi d'avis qu'il s'agit d'un bon moyen de mitiger les risques posés par leur utilisation de sites Internet qui collectent leurs renseignements personnels[155].

Certains témoins ont soulevé des doutes quant à la manière de réconcilier, d'une part, un droit à l'effacement des données et, d'autre part, la liberté d'expression garantie par la *Charte canadienne des droits et libertés*[156]. En effet, toute mesure visant à restreindre la capacité de publier de l'information sur Internet pourrait être considérée comme restreignant la liberté d'expression. On peut donc se demander s'il est possible de formuler un droit à l'effacement qui serait en mesure de protéger la vie privée sans porter atteinte à la liberté d'expression ou, du moins, qui constituerait une limite raisonnable à ce droit au titre de l'article 1 de la *Charte*. Sur ce plan, Robert Dickson, ancien commissaire à l'information et à la protection de la vie privée de la

153 ETHI, *Témoignages*, 1re session, 42e législature, 25 septembre 2017, 1545 (Kristjan Backman, président, Association nationale de destruction de l'information - Canada).

154 *Ibid.* (Owen Charters).

155 ETHI, *Témoignages*, 1re session, 42e législature, 6 avril 2017, 1635 (Paige Backman); ETHI, *Témoignages*, 1re session, 42e législature, 16 février 2017, 1725 (Valerie Steeves).

156 ETHI, *Témoignages*, 1re session, 42e législature, 1er février 2018, 0850 (Daniel Therrien).

Saskatchewan, a indiqué au Comité être d'avis qu'un droit à l'effacement ne résisterait pas à une contestation fondée sur la *Charte*[157].

Toutefois, d'autres témoins, dont M[e] Bernier, croient qu'un droit à l'effacement formulé de manière à se conformer à la *Charte* est possible :

> Je crois que le droit à l'effacement […] peut être formulé de façon à protéger la vie privée sans porter atteinte à la liberté d'expression, tout comme la *Loi sur la protection des Canadiens contre la cybercriminalité*. Dans ce texte législatif, nous criminalisons en quelque sorte une forme d'expression — par exemple, la publication non consensuelle d'une image intime sur le Web. Jusqu'à présent, la loi n'a pas été contestée ou déclarée inconstitutionnelle, car l'atteinte à la vie privée est si flagrante qu'elle ne s'applique pas à la liberté d'expression en général[158].

De plus, lors de son témoignage, le commissaire Therrien a établi une distinction utile entre la suppression d'informations factuelles – au sujet desquelles on peut au minimum exiger une certaine exactitude – et la suppression d'opinions, qui est une question qui relève beaucoup plus clairement de la liberté d'expression[159]. L'effacement, selon ce dernier, doit surtout viser la publication d'informations factuelles et peut constituer une solution plus rapide et plus efficace que d'autres recours traditionnels, comme une poursuite en diffamation devant les tribunaux[160]. Il faudra toutefois, comme l'indique le commissaire Therrien, s'assurer que tout processus d'effacement des données tienne compte des intérêts de la tierce partie les ayant publiés et de son droit à la liberté d'expression[161].

Un droit à l'effacement devrait néanmoins comporter plusieurs balises visant à assurer un équilibre adéquat entre la liberté d'expression et la protection de la vie privée. Par exemple, M[e] Bernier suggère d'éviter de laisser aux plateformes un pouvoir discrétionnaire de déterminer quand supprimer des informations, et qu'il revienne plutôt à un tribunal de déterminer si un affichage de données personnelles doit être supprimé en raison d'une atteinte à la vie privée[162]. Sans se prononcer quant à la pertinence du droit à l'effacement, M. Karanicolas du CLD a aussi fait part au Comité de

---

157 ETHI, *Témoignages*, 1re session, 42e législature, 14 février 2017, 1620 (Robert Dickson, consultant, ancien commissaire à l'information et à la protection de la vie privée de Saskatchewan, à titre personnel).

158 ETHI, *Témoignages*, 1re session, 42e législature, 14 février 2017, 1705 (Chantal Bernier).

159 ETHI, *Témoignages*, 1re session, 42e législature, 1er février 2018, 0950 (Daniel Therrien).

160 *Ibid.*

161 *Ibid.*, 0935

162 ETHI, *Témoignages*, 1re session, 42e législature, 14 février 2017, 1550 (Chantal Bernier).

l'importance d'une application régulière par un tribunal ou une autorité quasi judiciaire[163].

Qui plus est, afin de ne pas brimer la liberté d'expression, un droit limité à l'effacement devrait surtout viser les informations qui sont visées par la LPRPDE, c'est-à-dire la collecte, l'utilisation et la communication de renseignements personnels dans le cadre d'activités commerciales. Il ne s'agit pas de conférer aux individus un contrôle absolu leur permettant de gérer leur réputation en ligne[164]. Comme l'explique Florian Martin-Bariteau, professeur à la Faculté de droit de l'Université d'Ottawa, la reconnaissance d'un droit à l'effacement ne devrait pas permettre, par exemple, à des individus d'obliger des quotidiens à effacer des articles de presse ou de demander la suppression d'information contenue dans des fonds d'archives : « Je ne vois pas pourquoi aujourd'hui, parce que cela est facilité par les technologies, on autoriserait ce genre d'actions qui est d'effacer la mémoire[165]. » L'Association canadienne des archivistes (ACA) partage le même avis. Greg Kozak, qui témoignait au nom de l'ACA, considère qu'il est essentiel qu'un droit à l'effacement ne nuise pas indûment à la préservation de l'intégrité et de l'authenticité des documents publics et croit que « le critère utilisé pour déterminer si la réputation de quelqu'un est en danger doit être clair et suffisamment strict pour invalider les demandes frivoles ou illogiques[166] ».

Après avoir tenu compte de l'ensemble des témoignages entendus au cours de l'étude, le Comité est d'avis qu'il est important, afin de protéger la vie privée des Canadiens, de doter la LPRPDE d'un régime plus robuste en matière de suppression des renseignements personnels. Le Comité croit que les individus devraient de manière générale avoir le droit d'obtenir la suppression des renseignements personnels les concernant lorsque ces derniers mettent fin à une relation commerciale avec un fournisseur de services ou lorsque les renseignements ont été collectés, communiqués ou utilisés de manière contraire à la LPRPDE. Le Comité note d'ailleurs que le droit à l'effacement n'est pas un concept étranger à la LPRPDE, mais qu'il est important de le clarifier et de le renforcer. Tout en étant conscient des possibles conflits entre la reconnaissance d'un tel droit et la liberté d'expression, le Comité croit aussi qu'il est possible d'élargir quelque peu le droit à l'effacement en s'inspirant du RGPD de manière à mieux protéger la vie privée des Canadiens tout en étant respectueux de la *Charte*. En particulier, le Comité croit que, dans le cas des jeunes, l'exercice de mise en balance de

163 ETHI, *Témoignages*, 1re session, 42e législature, 23 février 2017, 1535 (Michael Karanicolas).

164 *Ibid.*

165 ETHI, *Témoignages*, 1re session, 42e législature, 23 février 2017, 1655 (Florian Martin-Bariteau).

166 ETHI, *Témoignages*, 1re session, 42e législature, 1er juin 2017, 1545 (Greg Kozak, représentant, Comité d'éthique, Association canadienne des archivistes).

la liberté d'expression et la protection de la vie privée devrait favoriser la mise en place d'un droit à l'effacement plus robuste, permettant la suppression des renseignements personnels qu'ils ont mis en ligne, que ce soit par eux-mêmes ou par le biais d'une organisation.

Par conséquent, le Comité recommande :

Recommandation 11 sur le droit à l'effacement :

Que le gouvernement du Canada envisage la mise en place, dans la *Loi sur la protection des renseignements personnels et les documents électroniques*, d'un encadrement du droit à l'effacement inspiré du modèle mis en place dans l'Union européenne qui, au minimum, inclurait un droit des jeunes d'obtenir l'effacement de renseignements qu'ils ont mis en ligne, que ce soit par eux-mêmes ou par le biais d'une organisation.

2. Le droit au déréférencement des données

Mis à part le droit à l'effacement, l'autre concept associé au droit à l'oubli est le droit d'obtenir le déréférencement des sites Internet contenant des renseignements personnels. Contrairement au droit à l'effacement, il ne s'agit pas de supprimer les données en question. Il s'agit plutôt de faire en sorte que ces renseignements ne soient plus référencés par les moteurs de recherche, comme Google, ce qui a pour effet de les rendre plus difficiles à trouver. Comme expliqué par Donna Bourne-Tyson, présidente de l'Association des bibliothèques de recherche du Canada (ABRC) :

> Concrètement, le délistage empêche le public d'accéder à de l'information en faisant une recherche à partir de mots clés; cependant, le contenu peut toujours être trouvé par un chercheur compétent et travaillant, qui peut aussi consulter des bases de données dont le contenu n'est pas indexé par les moteurs de recherche[167].

Tout comme le droit à l'effacement, le droit au déréférencement peut permettre à des individus de se dissocier d'erreurs de jugement commises il y a longtemps ou de publications rapportant de fausses accusations ou d'autres informations portant atteinte à leur réputation. Dans ces situations, le déréférencement rend plus difficile d'accès certaines pages Web publiées légalement par des tiers. Par exemple, un individu ayant obtenu un pardon pour une condamnation criminelle pourrait demander à ce que des articles de journaux faisant état de cet épisode de sa vie soient déréférencés de sorte qu'une recherche de son nom sur un moteur de recherche ne mène pas vers elles. Or, les articles demeureront disponibles sur Internet et accessibles par d'autres moyens,

167 ETHI, *Témoignages*, 1re session, 42e législature, 1er juin 2017, 1535 (Donna Bourne-Tyson, présidente, Association des bibliothèques de recherche du Canada).

et toute décision judiciaire portant sur cette affaire continuera d'être accessible sur les bases de données de jurisprudence (qui ne sont pas référencées dans les moteurs de recherche). Malgré le fait que l'information déréférencée demeurera dans le domaine public, il s'agit d'un moyen efficace de contrer la permanence de l'information. Comme l'indique Jane Bailey, professeure à la Faculté de droit de l'Université d'Ottawa : « dans la pratique, la plupart des gens se contenteront de faire une recherche Google. Si le lien ne peut plus être repéré par le moteur de recherche Google, il résultera de cette mesure une obscurité efficace et pratique, sans inconvénients[168]. »

Comme l'indique M[me] Steeves, il s'agit de mettre en équilibre, d'une part, l'intérêt individuel de pouvoir passer outre ses erreurs passées et, d'autre part, l'intérêt du public à avoir accès à certaines informations :

> Je pense que le droit à l'oubli comme on le conçoit en Europe concerne en fait la facilité d'accès, particulièrement quand l'intérêt public est en jeu. C'est donc une question d'équilibre. Mais même en ce qui concerne les dossiers des tribunaux, ces renseignements doivent être publics, puisque la justice doit être publique et il faut qu'on l'on puisse constater que justice a été rendue. Cependant, quand on a commencé à publier les dossiers matrimoniaux et que les gens effectuaient des recherches pour connaître le revenu de leurs voisins, cela a causé une kyrielle de problèmes; on a donc retiré ces renseignements d'Internet. Cependant, il s'agit toujours de renseignements publics et accessibles. C'est la facilité d'accès qui posait problème[169].

En 2014, le déréférencement a fait l'objet d'une décision de la Cour de justice de l'Union européenne (CJUE), l'arrêt *Google Spain c. AEPD et Mario Costeja González (Google Spain)*[170]. Dans cette affaire, la Cour a conclu que les moteurs de recherche comme Google doivent prendre en considération les demandes formulées par des individus en vue de faire retirer certaines pages apparaissant dans les résultats de recherches faites sur leur nom. La Cour, en interprétant la Directive 95/46/CE sur la protection des données personnelles (qui sera remplacée par le RGPD), a conclu que :

> [M]ême un traitement initialement licite de données exactes peut devenir, avec le temps, incompatible avec cette directive lorsque ces données ne sont plus nécessaires au regard des finalités pour lesquelles elles ont été collectées ou traitées. Tel est notamment le cas lorsqu'elles apparaissent inadéquates, qu'elles ne sont pas ou plus pertinentes ou sont excessives au regard de ces finalités et du temps qui s'est écoulé[171].

---

168 ETHI, *Témoignages*, 1re session, 42e législature, 25 septembre 2017, 1605 (Jane Bailey, professeure, Faculté de droit, Université d'Ottawa, à titre personnel).

169 ETHI, *Témoignages*, 1re session, 42e législature, 16 février 2017, 1700 (Valerie Steeves).

170 *Google Spain c. AEPD et Mario Costeja González*, ECLI:EU:C:2014:317.

171 *Ibid*., par. 93.

En réponse à cette décision, M. Karanicolas a indiqué au Comité qu'environ 348 000 demandes de déréférencement ont été faites à Google et qu'entre 150 000 et 170 000 sites Internet ont été retirés des résultats de recherche[172]. Dans le cas des demandes rejetées, il est possible pour les individus concernés de s'adresser aux tribunaux.

Au Canada, il n'existe pas de régime encadrant le déréférencement de manière explicite comme c'est le cas dans l'UE. Dans son projet de position, le CPVP a proposé une interprétation de la LPRPDE qui exigerait des moteurs de recherche un déréférencement dans certaines circonstances[173]. Or, en réponse à une question du Comité, le commissaire Therrien a convenu que cette interprétation n'est toutefois pas sans détracteurs et qu'il serait utile que la LPRPDE soit clarifiée à cet égard[174].

Cependant, comme l'indique M^me^ Stoddart, il existe certains régimes s'apparentant au déréférencement en droit canadien. Par exemple, lors de son témoignage, elle a fait valoir que, lorsque des individus obtiennent un pardon en droit pénal, l'accessibilité de cet antécédent judiciaire est réduite[175]. De plus, en 2017, dans l'arrêt *Google inc. c. Equustek Solutions inc.*, la Cour suprême du Canada a conclu qu'il est possible pour une cour de justice canadienne d'accorder une injonction interlocutoire mondiale contre un moteur de recherche afin de l'enjoindre à délister des sites Internet[176]. Il faut toutefois noter qu'il ne s'agissait pas d'une procédure judiciaire entamée en vertu de la LPRPDE ou d'un autre régime de protection des renseignements personnels, mais bien d'une demande d'injonction interlocutoire présentée dans le cadre d'un litige commercial relatif à l'acquisition illicite de renseignements confidentiels et de secrets commerciaux.

Le Comité a entendu plusieurs témoins sur la question de la reconnaissance possible d'un droit au déréférencement dans la LPRPDE. Sur le plan des mineurs, M^me^ Steeves a fait valoir devant le Comité qu'il s'agit d'une proposition « absolument essentielle[177] ». Il s'agit selon elle d'une revendication très importante auprès des jeunes, qui « craignent qu'une gaffe qu'ils ont faite à 16 ans leur cause des problèmes plus tard et que cela les suive toute leur vie[178] ». Pour sa part, M^me^ Bourne-Tyson de l'ABRC est d'avis qu'un droit

172 ETHI, *Témoignages*, 1re session, 42e législature, 23 février 2017, 1600 et 1610 (Michael Karanicolas).

173 CPVP, *Projet de position du Commissariat sur la réputation en ligne*, 26 janvier 2018.

174 ETHI, *Témoignages*, 1re session, 42e législature, 1er février 2018, 0900 (Daniel Therrien).

175 ETHI, *Témoignages*, 1re session, 42e législature, 23 mars 2017, 1650 (Jennifer Stoddart).

176 *Google Inc. c. Equustek Solutions Inc.*, 2017 CSC 34.

177 ETHI, *Témoignages*, 1re session, 42e législature, 16 février 2017, 1635 (Valerie Steeves).

178 *Ibid.*; ETHI, *Témoignages*, 1re session, 42e législature, 23 mars 2017, 1620 (Jennifer Stoddart).

limité au déréférencement pourrait être approprié, faisant valoir que « [l]a suppression de liens renvoyant à un délit commis par un mineur ou à des photos sexuellement explicites d'un simple citoyen sont de bons exemples d'application du droit à l'oubli », mais qu'il existe certaines zones grises qui doivent être prises en compte, par exemple de l'information concernant la faillite d'une entreprise[179]. M. Kozak, de l'ACA, croit que le déréférencement pourrait être une alternative intéressante à la suppression d'informations, car on préserverait le caractère public des informations en question tout en limitant le préjudice subi par les individus. Il croit aussi que le déréférencement permettrait aux informations ayant une certaine importance du point de vue archivistique de redevenir plus accessible lorsque le passage du temps aura anéanti le risque de préjudice :

> Dans les cas où le préjudice à la réputation diminue au fil du temps, et certainement avec le décès des personnes, voudrions-nous détruire complètement les listes ou les documents? La désindexation est peut-être une excellente façon d'atteindre cet équilibre qui consiste à dissimuler les renseignements pendant une période où ils sont sensibles, mais il faut être pleinement conscient du fait que ces renseignements font partie du domaine public et peuvent finir par revenir dans le domaine public dans un format plus accessible[180].

Les réserves présentées au Comité quant au modèle de droit au déréférencement qui existe en Europe ont surtout porté sur le fait qu'il revient au secteur privé de l'administrer. D'une part, Colin McKay, de Google Canada, a souligné devant le Comité que la décision dans l'affaire *Google Spain* a eu pour effet de forcer cette entreprise à « mettre sur pied un bureau et embaucher du personnel afin de pouvoir décider, en [s']appuyant sur les lois de 21 États différents, s'il faut accueillir ou rejeter une demande visant à retirer une URL de la liste des résultats de recherche[181] ». D'autre part, M. McKay a exprimé des doutes quant à la capacité d'un acteur privé d'atteindre un équilibre acceptable entre les intérêts en cause en tranchant sur des demandes de déréférencement :

> [I]l y a des gens qui ont eu un casier judiciaire dans leur jeunesse, qui ont fait preuve d'imprudence à l'université, et il y a aussi des gens qui ont été officiellement reconnus coupables de corruption ou de crimes violents, ou encore, tout simplement, des gens qui avaient l'habitude de faire connaître leurs opinions politiques ou personnelles en les

179 ETHI, *Témoignages*, 1re session, 42e législature, 1er juin 2017, 1535 (Donna Bourne-Tyson).

180 *Ibid.*, 1630 (Greg Kozak).

181 *Ibid.*, 1610 (Colin McKay, chef, Politiques publiques et relations gouvernementales, Google Canada).

> formulant gauchement. Il est difficile pour une entreprise du secteur privé de jouer le rôle de l'arbitre en cette matière[182].

M. Karanicolas abonde dans le même sens. Pour lui, les entreprises du secteur privé comme Google ne sont pas outillées pour tenir compte de l'intérêt du public, incluant la liberté d'expression, ce qui peut créer « une tendance à ce que l'information soit retirée chaque fois qu'il y a une plainte[183] ».

Le commissaire Therrien, pour sa part, reconnaît tout à fait la légitimité des réserves exprimées au sujet de l'administration d'un droit au déréférencement par des acteurs privés, mais invite à ne pas sous-estimer les avantages pratiques de cette solution[184]. Il souligne que ces organismes ont déjà des obligations, en vertu de la LPRPDE, qui nécessitent l'exercice de jugement et de mise en balance de divers intérêts, notamment sur le plan du respect du droit d'auteur[185]. Il ajoute : « Honnêtement, je ne vois pas en quoi le respect des lois fédérales sur la protection de la vie privée pour le secteur privé serait différent d'une infraction aux lois sur le droit d'auteur ou d'autres lois[186]. » Ainsi, le CPVP considère « approprié que les moteurs de recherche procèdent au premier examen d'une demande de déréférencement[187] ».

Un moyen de répondre aux réserves exprimées quant au rôle du secteur privé est d'adopter un cadre législatif rigoureux et d'en confier la mise en œuvre à une tierce partie objective et possédant une expertise suffisante. Par exemple, M[me] Bourne-Tyson et M. Karanicolas proposent de confier l'administration du droit au déréférencement à un tribunal[188]. Ce dernier, qui n'a toutefois pas pris position en faveur de la reconnaissance d'un droit au déréférencement, croit aussi qu'il serait important que le processus mis en place soit transparent, « ce qui comprend notamment le fait de mettre à la disposition des renseignements détaillés sur le fonctionnement et l'application des processus de prise de décisions[189] ». Afin de tenir compte de l'avantage pratique d'un rôle pour le secteur privé soulevé par le commissaire Therrien et afin de réduire le

---

182 *Ibid.*; ETHI, *Témoignages*, 1re session, 42e législature, 11 mai 2017, 1540 (Robert Ghiz, président et chef de direction, Association canadienne des télécommunications sans fil).

183 ETHI, *Témoignages*, 1re session, 42e législature, 23 février 2017, 1600 et 1610 (Michael Karanicolas).

184 ETHI, *Témoignages*, 1re session, 42e législature, 1er février 2018, 0905 (Daniel Therrien).

185 *Ibid.*, 0920.

186 *Ibid.*

187 CPVP, *Projet de position du Commissariat sur la réputation en ligne*, 26 janvier 2018.

188 ETHI, *Témoignages*, 1re session, 42e législature, 1er juin 2017, 1535 (Donna Bourne-Tyson); ETHI, *Témoignages*, 1re session, 42e législature, 23 février 2017, 1635 (Michael Karanicolas).

189 *Ibid.*

volume de demandes, un tel tribunal pourrait être une instance d'appel des décisions des moteurs de recherche.

Pour sa part, M[me] Bailey croit elle aussi qu'il est important que le processus mis en place afin de mettre en œuvre un droit au déréférencement soit transparent. Elle croit cependant que la mise en œuvre pourrait être effectuée par les fournisseurs de services si des mécanismes efficaces de reddition de compte sont mis en place :

> Je pense que l'idée d'un droit à l'oubli qui est une mesure concrète de désactivation des liens constitue en fait une réponse pratique intéressante, pourvu qu'il y ait une certaine compréhension et une obligation redditionnelle quant à la manière dont les fournisseurs de service prennent ces décisions lorsqu'il leur est demandé de le faire. Nous avons besoin d'une reddition de comptes, de transparence et de divulgation de leur part au sujet du nombre de demandes qu'ils reçoivent, des fondements de leurs prises de décision, du nombre de demandes acceptées et rejetées, de ce genre de choses. Je pense qu'il s'agirait là d'un droit à l'oubli applicable dans la pratique et offrant un certain degré de rectification[190].

Enfin, le CPVP a proposé, dans son projet de position, une liste non exhaustive de facteurs qui pourraient être pertinents lors de l'examen d'une demande de déréférencement :

- Si la personne concernée est une personnalité publique (p. ex. le titulaire d'une charge publique, un politicien ou un homme d'affaires bien en vue);
- Si les renseignements en jeu ont trait à une question faisant l'objet d'une controverse ou d'un débat public;
- Si les renseignements se rapportent à la vie privée d'une personne par opposition, par exemple, à sa vie professionnelle ou active;
- Si les renseignements concernent une infraction criminelle pour laquelle l'individu a obtenu une absolution, une réhabilitation ou une suspension de son casier judiciaire;
- Si les renseignements concernent un mineur […][191]

190 ETHI, *Témoignages*, 1re session, 42e législature, 25 septembre 2017, 1605 (Jane Bailey).

191 CPVP, *Projet de position du Commissariat sur la réputation en ligne*, 26 janvier 2018.

Le Comité croit que la mise en place d'un cadre juridique permettant aux individus de demander, dans certaines circonstances précises, le déréférencement de certaines informations préjudiciables les concernant est un bon moyen de protéger la réputation et la vie privée des Canadiens. Afin de préserver l'intérêt du public, incluant la liberté d'expression, ce cadre juridique devrait être élaboré de manière à prévoir un processus décisionnel rigoureux et transparent. De plus, le gouvernement du Canada devrait élaborer le droit au déréférencement en tenant compte de la situation particulière des mineurs.

Par conséquent, le Comité recommande :

Recommandation 12 sur le droit au déréférencement :

Que le gouvernement du Canada envisage la mise en place, dans la *Loi sur la protection des renseignements personnels et les documents électroniques*, d'un encadrement du droit au déréférencement et que ce droit soit explicitement reconnu à l'égard des renseignements personnels mis en ligne par un individu alors qu'il était mineur.

B. Destruction de renseignements personnels

Un autre sujet de préoccupation relatif à la protection des renseignements personnels abordé lors de l'étude a trait au manque de précisions dans la LPRPDE quant aux modalités de leur destruction, qu'il s'agisse de renseignements contenus en format papier ou sous une forme numérique.

M. Backman, de l'ANDI, considère qu'il s'agit d'un aspect négligé de la protection des renseignements personnels :

> En effet, les entreprises ne négligent que trop souvent la fin du cycle de vie de leurs documents. Nous constatons cela presque quotidiennement dans les médias, qui divulguent des renseignements intacts qu'ils trouvent dans des poubelles ou dans des ordinateurs mis au rancard à des fins de réutilisation ou de recyclage[192].

Or, la présence de renseignements personnels sur des produits recyclés ou toute autre manipulation négligente de renseignements personnels destinés à être détruits met en danger la vie privée des Canadiens :

> Dans le domaine de la destruction en général, nous avons vu au Canada de nombreux cas de divulgation illégale de dossiers personnels — notamment de dossiers de jeunes gens — due au fait que l'on n'en avait pas éliminé les renseignements personnels. Il s'agissait de dossiers de santé et de dossiers de clients de la Société de l'aide à

192 ETHI, *Témoignages*, 1re session, 42e législature, 25 septembre 2017, 1545 (Kristjan Backman).

> l'enfance. Une telle atteinte à la vie privée est dévastatrice pour les victimes, surtout pour les jeunes[193].

M. Martin-Bariteau a également indiqué qu'il « conviendrait néanmoins de rendre obligatoire, et non plus recommandable, la suppression des données dès lors qu'elles ne sont plus nécessaires ou à jour en encadrant plus strictement la rétention des données dans le temps[194] ».

Face à ce problème, l'ANDI revendique des modifications à la LPRPDE afin qu'elle exige la destruction et la définisse clairement. Dans son mémoire, l'ANDI propose une définition du mot « destruction », qui s'entendrait de « l'altération physique des documents de façon à les rendre inutiles et à rendre impossible la récupération de l'information, en tout ou en partie[195] ». Leur mémoire propose certaines autres modifications à la LPRPDE visant à préciser l'obligation de destruction, incluant une obligation d'inclure la destruction de renseignements personnels dans les politiques en matière de protection de la vie privée et imposant une obligation explicite de détruire les renseignements personnels dont une organisation n'a plus besoin[196].

Le Comité est d'avis qu'il est possible de protéger davantage la vie privée des Canadiens en renforçant les mécanismes prévus dans la LPRPDE en matière de destruction des renseignements personnels collectés par des entreprises et qui ne sont plus nécessaires ou qui doivent autrement être détruits. Sur ce plan, le Comité appuie les revendications formulées par l'ANDI qui visent à améliorer les modalités de la LPRPDE concernant la destruction des renseignements personnels.

Par conséquent, le Comité recommande :

Recommandation 13 sur la destruction des renseignements personnels :

Que le gouvernement du Canada envisage des modifications à la *Loi sur la protection des renseignements personnels et les documents électroniques* visant à renforcer et à préciser les obligations des organisations en matière de destruction des renseignements personnels.

193 *Ibid.*

194 ETHI, *Témoignages*, 1re session, 42e législature, 23 février 2017, 1550 (Florian Martin-Bariteau).

195 ETHI, Mémoire de l'ANDI, 8 février 2017, p. 6.

196 *Ibid.*

C. La protection de la vie privée dès la conception

Un moyen d'améliorer les mécanismes de protection des renseignements personnels prévus dans la LPRPDE est de mettre l'accent sur la protection de la vie privée à même la conception des services et des systèmes. La « protection de la vie privée dès la conception » est une approche qui vise justement à s'assurer que les considérations relatives à la protection de la vie privée soient prises en compte à toutes les étapes du développement, qu'il s'agisse du design, de la mise en marché ou de la mise hors service d'un produit. Cette approche fut notamment développée au Canada dans les années 1990 par Ann Cavoukian, ancienne commissaire à l'information et à la protection de la vie privée de l'Ontario[197].

La protection de la vie privée dès la conception vise à protéger les renseignements personnels par le biais de mesures agissant en amont et de manière préventive. Cette approche repose sur sept principes fondamentaux :

1) « Principe proactif et non réactif; prévention plutôt que correction » : L'objectif de la protection de la vie privée dès la conception est d'agir de manière préventive en prenant des mesures visant à réduire le risque d'atteinte à la sécurité de renseignements personnels[198].

2) « Le respect de la vie privée comme paramètre par défaut » : Les réglages par défaut de tout produit et services devraient favoriser la protection des renseignements personnels, de sorte que, sans intervention consciente de la part de l'utilisateur, sa vie privée sera protégée[199].

3) « Intégration du respect de la vie privée au niveau de la conception » : La protection des renseignements personnels doit être intégrée aux systèmes informatiques et aux pratiques d'affaires plutôt qu'un simple ajout périphérique[200].

4) « Pleine fonctionnalité – somme positive au lieu de somme nulle » : La protection de la vie privée dès la conception devrait être considérée

---

197 Commissaire à l'information et à la vie privée de l'Ontario, *Privacy by Design, The 7 Foundational Principles*, janvier 2011; voir généralement Ann Cavoukian, *Privacy by Design… Take the Challenge*. Commissaire à l'information et à la vie privée de l'Ontario, 2009.

198 Commissaire à l'information et à la vie privée de l'Ontario, *Privacy by Design, The 7 Foundational Principles*, janvier 2011.

199 *Ibid.*

200 *Ibid.*

comme une plus-value; il ne devrait pas être nécessaire de nuire à la mise en œuvre d'autres fonctionnalités afin de réaliser cet objectif[201].

5) « Sécurité de bout en bout – une protection complète pour le cycle de vie » : La protection des renseignements personnels doit être intégrée à l'ensemble du cycle de vie d'un système[202].

6) « Visibilité et transparence – assurer l'ouverture » : La transparence est importante afin de s'assurer que les systèmes et pratiques en place sont réellement en mesure de protéger la vie privée des utilisateurs; il doit toujours être possible de procéder à une vérification indépendante[203].

7) « Respect de la vie privée de l'utilisateur – maintenir une démarche centrée sur l'utilisateur » : Avant tout, la protection de la vie privée dès la conception doit prioriser les intérêts individuels[204].

Dans l'UE, les principes de la protection des renseignements personnels dès la conception ont été intégrés à l'article 25 du RGPD[205]. Comme l'explique Giovanni Buttarelli, le contrôleur européen de la protection des données :

> Les principes de protection de la vie privée dès la conception et de protection de la vie privée par défaut ne sont plus recommandés. Ils reposent maintenant sur des fondements juridiques et un énoncé clair des obligations respectives de chaque responsable. Ce qui veut dire que les systèmes doivent être conçus dans une approche conviviale et moins invasive. Les responsables ont des obligations, mais il existe un système pour que les concepteurs, les producteurs et les développeurs mettent ces principes en pratique[206].

Le Comité est d'avis que la protection de la vie privée dès la conception est un moyen efficace de protéger la vie privée et la réputation des Canadiens. Il s'agit d'une approche proactive et intégrée qui devrait être au cœur de toute révision de la LPRPDE.

Par conséquent, le Comité recommande :

---

201 *Ibid.*

202 *Ibid.*

203 *Ibid.*

204 *Ibid.*

205 Règlement général sur la protection des données, Reg 2016/679 (UE), art. 25; voir aussi le para. 78 du préambule.

206 ETHI, *Témoignages*, 1re session, 42e législature, 13 juin 2017, 1240 (Giovanni Buttarelli, contrôleur, Contrôleur européen de la protection des données).

Recommandation 14 sur la protection de la vie privée dès la conception :

Que la *Loi sur la protection des renseignements personnels et les documents électroniques* soit modifiée de sorte à faire de la protection de la vie privée dès la conception un principe central et incluant, dans la mesure du possible, les sept principes fondamentaux de ce concept.

PARTIE 4 : POUVOIRS D'EXÉCUTION DU COMMISSAIRE À LA PROTECTION DE LA VIE PRIVÉE

A. Rappel de la recommandation du Comité concernant l'application de la *Loi sur la protection des renseignements personnels*

Lors de son étude de la *Loi sur la protection des renseignements personnels* (LPRP) en 2016, le Comité a étudié différents modèles de surveillance qui pourraient convenir au CPVP pour l'application de la LPRP et a recommandé :

a) Que le gouvernement du Canada renforce la surveillance du droit d'accès en adoptant un modèle exécutoire dont les paramètres sont clairement et rigoureusement définis.

b) Que, afin de garantir l'utilisation la plus efficace des ressources, le gouvernement du Canada envisage des moyens de faire des gains d'efficacité tels que, par exemple, combiner les fonctions juridictionnelles du Commissariat à la protection de la vie privée du Canada et du Commissariat à l'information du Canada[207].

Bien que la LPRP et la LPRPDE prévoient des obligations différentes s'appliquant à des sphères différentes, l'une publique et l'autre privée, elles participent au même régime fédéral de protection de la vie privée administré par le CPVP. C'est pourquoi le Comité rappelle l'importance de prendre en compte les recommandations faites lors de l'étude de la LPRP au moment de considérer les recommandations concernant des modifications possibles au modèle de surveillance du CPVP pour l'application de la LPRPDE.

207 Chambre des communes, Comité permanent de l'accès à l'information, de la protection des renseignements personnels et de l'éthique (ETHI), *Protéger la vie privée des Canadiens : Examen de la* Loi sur la protection des renseignements personnels, quatrième rapport, 1re session, 42e législature, décembre 2016, recommandation 15, p. 40.

B. Position du Commissariat à la protection de la vie privée du Canada

Dans son mémoire à l'intention du Comité du 2 décembre 2016, le commissaire à la protection de la vie privée aborde la question du modèle de surveillance approprié dans le cadre de la LPRPDE. Le commissaire aborde l'opportunité d'amender la LPRPDE afin d'ajouter d'autres incitatifs à se conformer à la *Loi* :

> Il pourrait notamment s'agir de prévoir dans la loi des dommages-intérêts ou le pouvoir de rendre des ordonnances ou d'imposer des sanctions administratives pécuniaires (ou une combinaison de ces mesures), afin de maintenir la capacité du commissaire à protéger le droit des personnes à la vie privée dans une économie mondialisée où les menaces à la vie privée se multiplient[208].

En 2013, l'ancienne commissaire à la protection de la vie privée, M[me] Stoddart, avait d'ailleurs recommandé de « renforcer l'application de la *Loi* et encourager une plus grande conformité à celle-ci[209] ». Dans son mémoire, elle expliquait plus précisément comment les notions de dommages-intérêts, de pouvoirs d'ordonnance et de sanctions administratives pécuniaires s'appliqueraient à la LPRPDE.

Plus récemment, le renforcement des pouvoirs du commissaire était à l'étude lors des consultations menées par le CPVP sur le modèle de consentement de la LPRPDE. Aussi, le Projet de position du CPVP sur la réputation en ligne mentionne que la justification et les conclusions présentées dans le document du CPVP sur le consentement – c'est-à-dire de réclamer le pouvoir de rendre des ordonnances et d'imposer des amendes ainsi que l'officialisation du pouvoir de prendre des mesures proactives – s'appliquent également à la réputation en ligne[210].

C. Témoignages

1. Accorder de nouveaux pouvoirs au commissaire à la protection de la vie privée?

Steven Harroun, au nom du Conseil de la radiodiffusion et des télécommunications canadiennes, s'est dit convaincu que les sanctions administratives pécuniaires, de concert avec d'autres méthodes d'application de la loi, ont un effet dissuasif réel[211]. Il a

208 ETHI, Mémoire du Commissaire à la protection de la vie privée du Canada, 2 décembre 2016.

209 CPVP, *Arguments en faveur de la réforme de la* Loi sur la protection des renseignements personnels et les documents électroniques, mai 2013; *Schrems c. Data Protection Commissioner*, C-362/14, 6 octobre 2015.

210 CPVP, *Projet de position du Commissariat sur la réputation en ligne*, 26 janvier 2018.

211 ETHI, *Témoignages*, 1re session, 42e législature, 9 mai 2017, 1555 (Steven Harroun, chef de l'application de la Conformité et enquêtes, Conseil de la radiodiffusion et des télécommunications canadiennes).

recommandé au Comité de « fournir aux organismes d'application de la loi un éventail d'outils aussi large que possible afin qu'ils puissent adapter leur démarche en fonction des circonstances[212] ».

Krista Campbell, au nom d'Innovation, Sciences et Développement économique Canada, a estimé qu'au cours du prochain examen législatif de la LPRPDE, l'enjeu consistera à choisir entre un modèle d'ombudsman doté de pouvoirs semblables à ceux que possède le commissaire actuellement et un modèle différent[213].

> Si le commissaire veut disposer de pouvoirs d'ordonnance tout en conservant la possibilité de discuter ouvertement avec les chefs d'entreprise pour les inciter à demander de l'aide dès le départ pour la conception de nouveaux produits et services, on risque de s'interroger sur la teneur des priorités s'inscrivant dans le mandat principal du commissaire. Il faudrait donc procéder à un examen complet du commissariat et de la LPRPDE avant de décider d'octroyer de tels pouvoirs[214].

Dans l'attente de ce prochain examen législatif de la LPRPDE, le commissaire Therrien a précisé, lors de sa comparution du 16 février 2017, sa position concernant la possibilité d'accorder des pouvoirs d'exécution au commissaire à la protection de la vie privée. Selon lui, une combinaison du pouvoir exécutoire et de la capacité d'imposer des sanctions pécuniaires, encadrée par certains paramètres, serait la solution la plus efficace[215]. Lors de sa comparution du 1er février 2018, le commissaire Therrien a réitéré cette position et a ajouté que « si les organisations savent que leur interlocuteur a le pouvoir de prendre des ordonnances, les interactions seront plus efficaces[216] ».

À l'instar du commissaire, de nombreux témoins se sont prononcés en faveur de modifier le modèle d'ombudsman qui s'applique actuellement au commissaire afin

---

212 *Ibid.*

213 ETHI, *Témoignages*, 1re session, 42e législature, 9 mai 2017, 1605 (Krista Campbell, directrice générale, Direction générale des politiques numériques, Secteur du Spectre, Technologies de l'information et télécommunications, Innovation, Sciences et Développement économique Canada).

214 *Ibid.*

215 ETHI, *Témoignages*, 1re session, 42e législature, 16 février 2017, 1610 (Daniel Therrien).

216 ETHI, *Témoignages*, 1re session, 42e législature, 1er février 2018, 0855 (Daniel Therrien).

d'accorder à ce dernier des pouvoirs d'exécution[217]. Par exemple, John Lawford, du Centre pour la défense de l'intérêt public, a plaidé en faveur d'octroyer un véritable pouvoir d'application au commissaire qui inclurait le pouvoir discrétionnaire général d'imposer des sanctions administratives pécuniaires ou le pouvoir d'imposer des amendes[218]. Qui plus est, ce pouvoir d'imposer des amendes ne devrait pas, selon lui, être limité à des situations spécifiques, être réservé aux organismes judiciaires ou être assorti de contraintes[219].

M. Dickson, ancien commissaire à l'information et à la protection de la vie privée de la Saskatchewan, a fait valoir qu'un modèle exécutoire assorti du pouvoir d'imposer des pénalités permettrait d'accroître l'efficacité de la LPRPDE auprès des petites et moyennes entreprises (PME) et de créer des précédents juridiques[220].

Pour sa part, M. Martin-Bariteau a recommandé de prévoir dans la LPRPDE un montant maximum d'amende dissuasif, qui serait basé sur un pourcentage du chiffre d'affaires mondial de l'année précédente pour une organisation donnée et un second seuil chiffré, en retenant le montant le plus important[221]. Cette recommandation rejoint les dispositions du RGPD de l'UE, dont il est traité plus abondamment dans la prochaine partie du présent rapport. M. Martin-Bariteau a spécifié que les amendes ainsi prévues par la *Loi* devraient être payables au receveur général et qu'aucun pouvoir du commissaire, y compris ceux d'ordonnance et de sanction, ne devrait être limité à la réception préalable d'une plainte formelle[222]. Cependant, ces pouvoirs devraient, selon M. Martin-Bariteau, rester soumis à un possible contrôle judiciaire[223].

---

217 ETHI, *Témoignages*, 1re session, 42e législature, 16 février 2017, 1640 (Vincent Gogolek); ETHI, *Témoignages*, 1re session, 42e législature, 21 février 2017, 1535 (Drew McArthur); ETHI, *Témoignages*, 1re session, 42e législature, 21 mars 2017, 1605 (Micheal Vonn, directrice de la politique, Association des libertés civiles de la Colombie-Britannique), ETHI, *Témoignages*, 1re session, 42e législature, 21 mars 2017, 1620 (Michael Geist); ETHI, *Témoignages*, 1re session, 42e législature, 4 avril 2017, 1630 (Ian Kerr); ETHI, *Témoignages*, 1re session, 42e législature, 4 avril 2017, 1645 (Vincent Gautrais); Option consommateurs, Mémoire, *La révision de la* Loi sur la protection des renseignements personnels et les documents électroniques *: Tout vient à point…*, 11 mai 2017, recommandation 1- n), p. 15, ETHI, *Témoignages*, 1re session, 42e législature, 16 mai 2017, 1600 (Dennis Hogarth); ETHI, *Témoignages*, 1re session, 42e législature, 1er juin 2017, 1645 (Greg Kozak).

218 ETHI, *Témoignages*, 1re session, 42e législature, 14 février 2017, 1600 (John Lawford).

219 *Ibid.*

220 ETHI, *Témoignages*, 1re session, 42e législature, 14 février 2017, 1620 (Robert Dickson).

221 ETHI, *Témoignages*, 1re session, 42e législature, 23 février 2017, 1550 (Florian Martin-Bariteau).

222 ETHI, *Témoignages*, 1re session, 42e législature, 14 février 2017, 1555 (Chantal Bernier). Me Bernier a fait une recommandation semblable, en spécifiant que l'amende en question devrait équivaloir à un pourcentage des recettes annuelles de l'organisation.

223 ETHI, *Témoignages*, 1re session, 42e législature, 23 février 2017, 1550 (Florian Martin-Bariteau).

M. Martin-Bariteau a également recommandé d'accorder aux individus des droits d'action statutaires, non soumis à une plainte préalable au CPVP et bénéficiant de dommages-intérêts statutaires, pour faire respecter les obligations prévues à la LPRPDE ou pour obtenir réparation le cas échéant[224]. M. Israel, de la CIPPIC, a fait des recommandations qui vont dans le même sens, en plus de recommander d'accorder au commissaire le pouvoir d'imposer des obligations détaillées de production de rapports à des fins de transparence dans les différents secteurs dont la responsabilité lui échoit[225].

En ce qui concerne les dommages-intérêts accordés en vertu de la LPRPDE, M[me] Scassa a expliqué que

> La LPRPDE ne fournit pas d'orientations générales sur les jugements en dommages-intérêts. La Cour fédérale s'est montrée extrêmement conservatrice à cet égard pour des infractions à la LPRPDE, et il est peu probable qu'il y ait d'autres effets dissuasifs que de dissuader les personnes qui se battent pour défendre leur droit à la vie privée. Il conviendrait d'accorder une attention particulière à l'établissement de paramètres pour des dommages non pécuniaires aux termes de la LPRPDE. À tout le moins, cela aiderait les plaidants non représentés à comprendre les limites de tout recours possible[226].

M[me] Scassa a également recommandé que le commissaire ait le pouvoir général d'imposer des amendes aux organisations dans des situations de non-conformité importante ou systémique[227]. Dans le même ordre d'idées, M. Israel a plaidé en faveur d'accorder au commissaire le pouvoir d'imposer des restrictions adaptées au contexte[228]. Selon lui, « le modèle fondé sur des recommandations et le recours à une deuxième instance pour l'application de la LPRPDE est complètement déconnecté de la réalité moderne des régimes de protection des données[229] ».

Colin Bennett, professeur de sciences politiques à l'Université de Victoria, a recommandé pour sa part d'accorder au commissaire à la protection de la vie privée du Canada les mêmes pouvoirs que ceux dont dispose le commissaire à l'information et à la protection de la vie privée de la Colombie-Britannique[230]. Selon M. Bennett, le commissaire à la protection de la vie privée du Canada doit disposer de tous les outils

---

224 *Ibid.*

225 ETHI, *Témoignages*, 1re session, 42e législature, 23 mars 2017,1635 (Tamir Israel).

226 ETHI, *Témoignages*, 1re session, 42e législature, 23 février 2017, 1545 (Teresa Scassa).

227 *Ibid.*

228 ETHI, *Témoignages*, 1re session, 42e législature, 23 mars 2017,1630 (Tamir Israel).

229 *Ibid.*, 1635.

230 ETHI, *Témoignages*, 1re session, 42e législature, 21 mars 2017, 1640 (Colin Bennett, professeur de sciences politiques, Université de Victoria).

disponibles en matière de protection des renseignements personnels, dont des codes de pratique, des sceaux de protection et des normes et des évaluations des facteurs relatifs à la vie privée. Par conséquent, il a recommandé :

> qu'il soit expressément reconnu à l'article 24 de la LPRPDE que le commissaire peut encourager l'utilisation de ce type d'outils et, dans certains cas, oblige l'adoption de ces mécanismes de reddition de comptes par les entreprises canadiennes et leurs associations commerciales. Plus particulièrement, il y a la protection de la vie privée dès la conception et la protection par défaut[231].

2. Un point de vue européen sur la question des amendes

M. Buttarelli, le contrôleur européen de la protection des données, a expliqué au Comité que, selon lui, toutes les violations ne peuvent être traitées de la même façon : la gravité des violations doit être prise en compte pour établir le caractère raisonnable et crédible des sanctions qui y sont liées[232]. Selon lui, « [n]ous devons éviter un système où les amendes ne sont qu'un poste budgétaire pour une grande société. Nous devons augmenter le montant des amendes quand il le faut, en fonction de l'argent et de l'énergie que le contrôleur a consacrés à l'affaire[233] ».

3. L'application de la loi à la situation particulière des enfants

En ce qui concerne les enfants, Repaires jeunesse du Canada a recommandé, dans son mémoire à l'intention du Comité, de donner au CPVP « le pouvoir d'appliquer les nouveaux règlements portant sur la protection des renseignements personnels des enfants[234] ». Lors de son témoignage du 25 septembre 2017, M. Charters, de RJC, a

---

231 *Ibid.* L'article 24 de la LPRPDE concerne la promotion de l'objet de la partie 1 de la *Loi* – qui porte sur la protection des renseignements personnels dans le secteur privé – et prévoit que :

« Le commissaire :

a) offre au grand public des programmes d'information destinés à lui faire mieux comprendre la présente partie et son objet;

b) fait des recherches liées à la protection des renseignements personnels — et en publie les résultats —, notamment toutes telles recherches que le ministre de l'Industrie demande;

c) encourage les organisations à élaborer des politiques détaillées — notamment des codes de pratiques — en vue de se conformer aux articles 5 à 10;

d) prend toute autre mesure indiquée pour la promotion de l'objet de la présente partie. »

232 ETHI, *Témoignages*, 1re session, 42e législature, 13 juin 2017, 1320 (M. Giovanni Buttarelli, contrôleur, Contrôleur européen de la protection des données).

233 *Ibid.*

234 Repaires jeunesse du Canada, Mémoire, *Protéger les renseignements personnels des enfants en ligne*, mars 2017, recommandation 4, p. 3.

précisé sa pensée en affirmant qu'« [i]l ne suffit pas de créer des lois. Les entreprises et les sites doivent être surveillés et tenus responsables du respect de ces dispositions[235] ».

Comme exemple de règles qu'il souhaite voir ajouter à la LPRPDE afin d'y inclure explicitement le droit des enfants à la protection de la vie privée, M. Charters a mentionné la *Children's Online Privacy Protection Act* des États-Unis – qui exige le consentement parental pour recueillir les renseignements personnels des enfants de moins de 13 ans – et le RGPD, qui exige le consentement d'un parent ou d'un tuteur pour accéder à des services en ligne pour les enfants de moins de 16 ans, ou moins, pourvu que l'âge prévu soit d'au moins 13 ans[236].

4. Le point de vue des organisations assujetties à la *Loi sur la protection des renseignements personnels et les documents électroniques*

Examinant les pouvoirs du commissaire à la protection de la vie privée par l'autre bout de la lorgnette, plusieurs témoins se sont prononcés en faveur du maintien du modèle de l'ombudsman, contre le fait d'accorder des pouvoirs d'exécution au commissaire, ou encore en faveur d'encadrer rigoureusement ces pouvoirs d'exécution[237]. Par exemple, Mme Duval, au nom de l'ACCAP, a recommandé de continuer d'utiliser le modèle de l'ombudsman « puisqu'il permet un bon équilibre entre les droits des individus en matière de protection des renseignements personnels et les droits des organisations d'utiliser ces renseignements de façon légitime et raisonnable dans un contexte commercial[238] ».

---

235 ETHI, *Témoignages*, 1re session, 42e législature, 25 septembre 2017, 1545 (M. Owen Charters, président-directeur général, Repaires jeunesse du Canada).

236 *Ibid.*, 1655.

237 ETHI, *Témoignages*, 1re session, 42e législature, 21 mars 2017, 1630 (David Fraser); ETHI, *Témoignages*, 1re session, 42e législature, 6 avril 2017, 1640 (Paige Backman); ETHI, *Témoignages*, 1re session, 42e législature, 6 avril 2017, 1610 (Alex Cameron, associé et président, Protection de l'information et de la vie privée, Fasken Martineau DuMoulin LLP); ETHI, *Témoignages*, 1re session, 42e législature, 11 mai 2017, 1540 (Robert Ghiz); ETHI, *Témoignages*, 1re session, 42e législature, 11 mai 2017, 1550 (Wally Hill); ETHI, *Témoignages*, 1re session, 42e législature, 11 mai 2017, 1650 (David Elder); ETHI, *Témoignages*, 1re session, 42e législature, 16 mai 2017, 1550 (Robert Watson); ETHI, *Témoignages*, 1re session, 42e législature, 16 mai 2017, 1625 (André Leduc, vice-président, Relations gouvernementales et politiques, Association canadienne de la technologie de l'information); ETHI, *Témoignages*, 1re session, 42e législature, 16 mai 2017, 1610 (Scott Smith, directeur, Propriété intellectuelle et politique d'innovation, Chambre de commerce du Canada); ETHI, *Témoignages*, 1re session, 42e législature, 30 mai 2017, 1550 (Randy Bundus); ETHI, *Témoignages*, 1re session, 42e législature, 30 mai 2017, 1600 (Adam Kardash); ETHI, *Témoignages*, 1re session, 42e législature, 1er juin 2017, 1550 (Jason McLinton, vice-président, Division Alimentation et Affaires réglementaires, Conseil canadien du commerce de détail); ETHI, *Témoignages*, 1re session, 42e législature, 1er juin 2017, 1655 (Colin McKay).

238 ETHI, *Témoignages*, 1re session, 42e législature, 30 mai 2017, 1540 (Anny Duval).

Quant à elle, M[e] Bernier a fait remarquer que la comparaison des pouvoirs d'exécution du CPVP avec ceux des autres commissariats dans le monde indique qu'une mise à niveau semble s'imposer, mais selon certains paramètres[239]. Elle a recommandé au Comité d'explorer la possibilité d'accorder au commissaire le pouvoir d'imposer des amendes, mais seulement si une preuve de négligence de la part de l'organisation visée existe. Selon M[e] Bernier,

> l'imposition de sanctions n'est pas nécessairement néfaste pour le secteur privé, puisqu'en fait, elle peut rétablir l'équité entre les organisations diligentes qui affectent, elles, en amont, les ressources nécessaires à la protection des renseignements, et celles négligentes qui, ne l'ayant pas fait, payent l'amende en aval. Beaucoup de représentants d'organisations diligentes vous diront: « Merci. Vous venez d'équilibrer les règles du jeu[240]. »

En matière de comparaison des pouvoirs d'exécution du CPVP avec ceux des autres commissariats dans le monde, l'ancienne commissaire Stoddart, dans son mémoire de 2013, rappelait que la Federal Trade Commission des États-Unis a négocié de nombreux règlements financiers à la suite d'atteintes à la vie privée[241].

> Les autorités de protection des données du Royaume-Uni, de l'Irlande, de la Nouvelle-Zélande et de l'Espagne ont également le pouvoir de rendre des ordonnances, le Royaume-Uni et l'Espagne disposant en outre de la capacité d'imposer une amende aux organisations. Au Royaume-Uni, ces pouvoirs d'application de la loi plus grands n'ont pas empêché la mise en place d'une approche de type ombudsman. Des amendes sont en effet imposées seulement lorsqu'une méthode plus douce n'a pas fonctionné[242].

M[me] Stoddart mentionnait également que la *Privacy Act* australienne avait été modifiée à l'époque de son mémoire afin d'accorder au commissaire le pouvoir d'accepter des engagements exécutoires et de s'adresser à la Cour fédérale pour imposer des amendes de plus de 1 million de dollars (australiens) pour une entreprise[243].

Appelée à fournir des exemples d'autres administrations qui ont le pouvoir d'imposer des amendes et dont le Canada pourrait s'inspirer, M[e] Bernier a mentionné le Royaume-Uni, où les amendes vont jusqu'à 25 000 livres, et la France, où elles peuvent s'élever

---

239 ETHI, *Témoignages*, 1re session, 42e législature, 14 février 2017, 1555 (Chantal Bernier).

240 *Ibid.*

241 CPVP, *Arguments en faveur de la réforme de la* Loi sur la protection des renseignements personnels et les documents électroniques, 23 mai 2013, p. 7.

242 *Ibid.*

243 *Ibid.*

jusqu'à 300 000 euros[244]. À propos des ordonnances rendues dans ces deux pays, M. Hogarth a argué que si elles peuvent sembler un peu extrêmes, elles sont très efficaces pour obtenir la conformité avec les exigences qu'elles cherchent à faire respecter[245].

Les nouvelles sanctions qui entreront bientôt en vigueur dans l'UE en vertu du RGPD sont abordées dans la prochaine partie du présent rapport.

Rejoignant M. Martin-Bariteau sur ce point, M^e^ Bernier a également recommandé que ces amendes soient payables au receveur général, afin d'éviter tout conflit d'intérêts, et que leur imposition soit assortie d'un droit d'appel à la Cour fédérale. Elle s'est également dite favorable à ce que l'amende en question soit calculée selon un pourcentage des revenus annuels de l'organisation, comme dans le cas du nouveau règlement européen, parce que l'utilisation de renseignements personnels fait partie des profits. M^e^ Bernier a fourni l'explication suivante à cet égard :

> Du coup, une mauvaise utilisation des renseignements personnels devrait faire partie des pertes financières. Il y a là une logique, selon moi, à reconnaître la valeur financière des renseignements personnels. Ensuite, cela permet un arrimage avec l'investissement nécessaire en amont. Enfin, cela laisserait la question des dommages-intérêts aux recours civils, comme il se doit[246].

Après avoir exprimé la crainte du risque que l'imposition de dommages-intérêts ou d'autres sanctions freine l'innovation des entreprises, M^e^ Gratton, a recommandé que « les pouvoirs exécutoires, les pénalités et les dommages-intérêts ne devraient entrer en jeu qu'une fois qu'il a été clairement établi que la pratique est illégale et que l'organisation fautive a refusé d'apporter les correctifs nécessaires après avoir été avisée de la situation[247] ».

Pour sa part, M. Karanicolas s'est dit en faveur d'accorder des pouvoirs d'enquête plus vastes au CPVP pour promouvoir des pratiques exemplaires en matière de gestion de l'information et de la sécurité, mais n'est pas convaincu qu'il faille donner au commissaire le pouvoir de rendre des ordonnances[248]. Cette réticence s'explique, selon lui, par le fait que certaines questions se posent à propos de l'équité procédurale pour

244 ETHI, *Témoignages*, 1re session, 42e législature, 14 février 2017, 1725 (Chantal Bernier).

245 ETHI, *Témoignages*, 1re session, 42e législature, 16 mai 2017, 1710 (Dennis Hogarth).

246 ETHI, *Témoignages*, 1re session, 42e législature, 14 février 2017, 1555 (Chantal Bernier).

247 ETHI, *Témoignages*, 1re session, 42e législature, 14 février 2017, 1620 (Éloïse Gratton).

248 ETHI, *Témoignages*, 1re session, 42e législature, 23 février 2017, 1530 et 1605 (Michael Karanicolas).

les enquêtes ainsi qu'au fait que le commissaire a affirmé que la plupart de ses recommandations sont respectées par les organisations[249].

M[me] Morin, au nom de l'ABC, a recommandé « le maintien du modèle de protecteur du citoyen en l'absence de preuve d'un besoin impératif de modifier les pouvoirs de contrainte du CPVP[250] ». Elle a également recommandé de modifier la LPRPDE afin d'autoriser le CPVP « à produire des avis préalables non exécutoires à la demande d'organisations envisageant de nouveaux programmes, de nouvelles technologies ou méthodes, ou des transactions précises[251] ». Par ailleurs, M[me] Morin a invité à la prudence en attendant l'interprétation qui sera donnée au nouveau pouvoir du CPVP de conclure des ententes de conformité contraignantes avec les organisations en ayant recours aux tribunaux, et l'utilisation qui en sera faite, ainsi que le nouveau régime d'obligation de signalement des atteintes qui permettra l'imposition d'amendes, lorsqu'il entrera en vigueur en 2018[252].

Abondant dans le même sens que M[me] Morin sur cette question, Molly Reynolds, associée principale chez Torys LLP, a recommandé d'apporter des modifications à la LPRPDE afin de prévoir la possibilité pour le CPVP de rendre des décisions anticipées[253]. Selon elle, quatre conséquences importantes découleraient de ce pouvoir de rendre des décisions anticipées en matière de conformité. La décision anticipée permettrait ainsi :

- de mieux protéger les Canadiens;
- au CPVP de développer une connaissance approfondie des nouvelles technologies;
- d'accroître la prévisibilité pour toutes les parties;
- d'aider le secteur privé à mieux évaluer les risques[254].

249 *Ibid.*

250 ETHI, *Témoignages*, 1re session, 42e législature, 23 mars 2017, 1640 (Suzanne Morin).

251 *Ibid.*, 1645.

252 *Ibid.*

253 ETHI, *Témoignages*, 1re session, 42e législature, 6 avril 2017, 1620 (Molly Reynolds, associée principale, Torys LLP).

254 *Ibid.*

Mme Reynolds a précisé que ces décisions anticipées ne devraient pas être contraignantes[255].

David Young, de chez David Young Law, a argué que le modèle en place actuellement, au sein duquel le commissaire joue le rôle d'un médiateur, fonctionne bien[256]. Il s'est toutefois montré ouvert à l'idée d'accorder au commissaire le pouvoir de rendre des ordonnances « s'il est établi que le présent modèle n'offre pas les outils nécessaires pour assurer un contrôle d'application efficace[257] ». Selon M. Young, le fait de donner au commissaire le pouvoir d'imposer des sanctions pécuniaires « dénaturerait considérablement ses pouvoirs actuels et ne cadrerait pas avec le modèle de l'ombudsman[258] ». Cependant, il a évoqué la possibilité de prévoir des sanctions pécuniaires pour des infractions comme une violation intentionnelle de la loi, qui s'harmoniseraient avec la nouvelle infraction prévue en cas de manquement à l'obligation de déclarer les atteintes aux mesures de sécurité d'une organisation[259].

À la lumière de l'ensemble des témoignages entendus et des mémoires reçus, le Comité considère que le besoin d'accorder au commissaire à la protection de la vie privée des pouvoirs d'exécution pour l'application de la LPRPDE a été démontré. Pour cette raison, le Comité recommande de se servir du système en place au Royaume-Uni comme modèle et recommande :

Recommandation 15 sur les pouvoirs d'exécution du commissaire à la protection de la vie privée :

Que la *Loi sur la protection des renseignements personnels et les documents électroniques* soit modifiée afin d'accorder au commissaire à la protection de la vie privée des pouvoirs d'exécution, incluant le pouvoir de rendre des ordonnances et le pouvoir d'imposer des amendes en cas de non-respect de ces ordonnances.

En plus de recommander que le commissaire ait le pouvoir d'imposer des amendes, M[me] Stoddart a recommandé que la LPRPDE accorde au commissaire le pouvoir de choisir les plaintes sur lesquelles il souhaite mener une enquête[260]. Ce pouvoir de choisir serait accompagné de vastes pouvoirs de vérification ou du pouvoir de lancer lui-même une

255 *Ibid.*, 1625.

256 ETHI, *Témoignages*, 1re session, 42e législature, 4 avril 2017, 1615 (David Young).

257 *Ibid.*

258 *Ibid.*

259 *Ibid.*

260 ETHI, *Témoignages*, 1re session, 42e législature, 23 mars 2017, 1620 (Jennifer Stoddart).

enquête. Elle considère également qu'une plus grande souplesse devrait être accordée au CPVP, afin d'élargir son éventail d'outils réglementaires[261].

Souscrivant à cette recommandation de M[me] Stoddart, le Comité recommande :

Recommandation 16 sur les pouvoirs du commissaire à la protection de la vie privée en matière d'audit :

Que la *Loi sur la protection des renseignements personnels et les documents électroniques* soit modifiée afin d'accorder au commissaire à la protection de la vie privée des pouvoirs étendus en matière d'audit, incluant le pouvoir de choisir les plaintes sur lesquelles enquêter.

PARTIE 5 : CARACTÈRE ADÉQUAT DE LA *LOI SUR LA PROTECTION DES RENSEIGNEMENTS PERSONNELS ET LES DOCUMENTS ÉLECTRONIQUES* AU REGARD DU *RÈGLEMENT GÉNÉRAL SUR LA PROTECTION DES DONNÉES DE L'UNION EUROPÉENNE*

A. Le *Règlement général sur la protection des données* de l'Union européenne

En 1995, l'UE a adopté une directive – devenue applicable en 1998 – assurant la protection des renseignements personnels tout en permettant leur libre circulation au sein de l'UE. La directive oblige tous les pays membres à s'y conformer en adoptant une loi sur la protection des données ou en modifiant leur législation existante. L'article 25 de la directive étend la portée de celle-ci au-delà de l'UE en interdisant aux pays membres (et aux entreprises s'y trouvant) de transférer des renseignements personnels à tout pays non membre dont les lois n'offrent pas un niveau de protection adéquat à ces renseignements[262].

La directive sera remplacée en mai 2018 lorsque le RGPD sera directement applicable sur le territoire de l'UE. En vertu du RGPD, l'UE devra évaluer « le caractère adéquat des

261 *Ibid.*, 1625.

262 Parlement européen, Conseil de l'Union européenne, *Directive 95/46/CE du Parlement européen et du Conseil, du 24 octobre 1995, relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données*, 24 octobre 1995.

mesures de protection prévues par la LPRPDE[263] ». Dans son mémoire au Comité du 2 décembre 2016, le commissaire explique que le RGPD « renferme certaines dispositions absentes de la Directive actuelle et de la LPRPDE concernant, par exemple, la portabilité des données, l'effacement de données et la protection de la vie privée dès la conception et par défaut[264] ».

Les institutions de l'UE ont résumé les dispositions principales du RGPD en les divisant en deux catégories : les droits des citoyens et les règles pour les entreprises[265]. En ce qui concerne les droits des citoyens, les institutions de l'UE ont affirmé que le RGPD « renforce les droits existants, octroie de nouveaux droits et accorde aux citoyens un meilleur contrôle sur leurs données à caractère personnel[266] », en prévoyant notamment :

- un **meilleur accès à leurs données** — y compris en fournissant plus d'informations sur la manière dont les données sont traitées et en garantissant que ces informations sont disponibles de manière claire et compréhensible;

- un **nouveau droit à la portabilité des données** — destiné à faciliter le transfert de données à caractère personnel entre prestataires de services;

- un **droit d'effacement (« droit à l'oubli »)** plus clair — lorsqu'une personne ne souhaite plus que ses données soient traitées et qu'il n'existe pas de motif légitime de les conserver, les données seront effacées;

- le **droit de savoir quand ses données à caractère personnel ont été piratées** — les entreprises et les organisations devront informer sans délai les personnes en cas de violation grave des données. Elles devront également en informer les autorités de contrôle de la protection des données compétentes[267].

263 ETHI, Mémoire du Commissaire à la protection de la vie privée du Canada, 2 décembre 2016; Conseil de l'Union européenne, *Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données)*, art. 103 à 108.

264 ETHI, Mémoire du Commissaire à la protection de la vie privée du Canada, 2 décembre 2016.

265 Europa, *Législation et publications de l'UE*, Protection des données à caractère personnel (à partir de 2018).

266 *Ibid.*

267 *Ibid*.

En ce qui concerne les règles pour les entreprises, les institutions de l'UE ont affirmé que le RGPD « est conçu pour créer des opportunités commerciales et encourager l'innovation[268] » grâce, entre autres, aux mesures suivantes :

- **un ensemble unique de règles européennes** — une législation européenne unique pour la protection des données représenterait une économie de 2,3 milliards d'euros par an;

- un **délégué à la protection des données**, chargé de la protection des données, sera désigné par les autorités publiques et par les entreprises qui traitent les données à grande échelle;

- un **guichet unique** — les entreprises ne doivent traiter qu'avec une seule autorité de contrôle (dans le pays de l'UE dans lequel elles sont principalement implantées);

- des **règles européennes pour les entreprises non européennes** — les entreprises basées en dehors de l'UE doivent appliquer les mêmes règles quand elles proposent des services ou des biens, ou suivent le comportement des personnes au sein de l'UE;

- des **règles propices à l'innovation** — une garantie que les mesures de protection des données sont intégrées dans les produits et les services depuis les premières étapes du développement (protection des données dès la conception et par défaut);

- des **techniques respectueuses de la vie privée** telles que la **pseudonymisation** (lorsque les champs d'identification dans un enregistrement de données sont remplacés par un ou plusieurs identifiants factices) et le **chiffrement** (lorsque les données sont codées de manière telle que seules les parties autorisées peuvent les lire);

- la **suppression des notifications** — les nouvelles règles de protection des données supprimeront la plupart des obligations de notification et les coûts associés à ces obligations. Un des objectifs du règlement sur la protection des données consiste à supprimer les obstacles au libre flux des données à caractère personnel au sein de l'UE. Il permettra aux entreprises de se développer plus facilement;

- des **analyses d'impact** — les entreprises devront effectuer des analyses d'impact lorsque le traitement des données peut engendrer un risque élevé pour les droits et libertés des personnes physiques;

268 *Ibid*.

- la **tenue des registres** — les PME ne sont pas obligées de tenir des registres des activités de traitement, à moins que le traitement ne soit régulier ou susceptible d'engendrer un risque pour les droits et libertés de la personne dont les données sont traitées[269].

De plus, le RGPD prévoit des mesures sévères d'application de la loi, comme des amendes administratives reliées aux violations les plus graves qui peuvent s'élever jusqu'à 20 millions d'euros ou jusqu'à 4 % du chiffre d'affaires annuel mondial total de l'exercice financier précédent de l'organisation visée, en retenant le montant le plus élevé[270]. En vertu du RGPD, les autorités de contrôle européennes auront également des pouvoirs d'enquête – dont celui de procéder à des audits sur la protection des données des organisations visées – et le pouvoir d'imposer aux organisations une limitation temporaire ou définitive, y compris une interdiction, du traitement de renseignements personnels[271].

Le commissaire mentionne également dans son mémoire du 2 décembre 2016 l'incidence de la décision *Schrems c. Data Protection Commissioner* dans laquelle la CJUE a statué que la loi des États-Unis ne comporte pas un niveau adéquat de protection pour les données personnelles[272]. Cela a eu pour effet d'invalider le cadre de l'accord *Safe Harbour* entre l'UE et les États-Unis[273]. La décision *Schrems* aborde la notion de protection adéquate :

> [L]a décision Schrems exige une approche plus globale de la protection adéquate que celle qui était en place au moment où la LPRPDE a été déclarée « adéquate ». La notion de protection adéquate ne se limite plus à l'examen des règles permettant de protéger les renseignements personnels dans la sphère commerciale – il faut aussi examiner attentivement les mesures de protection des droits dans les lois et les pratiques relatives à la sécurité nationale et à l'application des lois[274].

---

269 *Ibid*.

270 *Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données)*, art. 83.

271 *Ibid*., art. 58.

272 ETHI, *Mémoire du Commissaire à la protection de la vie privée du Canada*, 2 décembre 2016.

273 L'accord *Safe Harbour* constituait un outil pour les entreprises du secteur privé de l'UE afin de s'assurer que les transferts des données personnelles de citoyens de l'UE vers les États-Unis se déroulaient selon un niveau de protection jugé adéquat en vertu de la Directive. Il est à noter que l'UE et les États-Unis sont parvenus à une nouvelle entente, le *Bouclier vie privée UE–États-Unis*; Commission européenne, *La Commission européenne et les États-Unis s'accordent sur un nouveau cadre pour les transferts transatlantiques de données, le « bouclier vie privée UE–États-Unis »*, communiqué, 2 février 2016.

274 CPVP, *Le dilemme du consentement : Allocution prononcée à la conférence internationale Privacy Laws and Business*, 5 juillet 2016.

Ainsi, selon le commissaire, en raison des différences entre la LPRPDE et le RGPD et des conséquences de la décision *Schrems*, la réévaluation du caractère adéquat de la LPRPDE « est un enjeu urgent susceptible d'avoir de profondes répercussions sur les relations commerciales du Canada avec l'Union européenne[275] ».

B. Témoignages

1. À la recherche de l'adéquation

Lors de son témoignage du 16 février 2017, le commissaire a invité les membres du Comité à garder en tête durant leur étude l'adéquation de la LPRPDE par rapport au RGPD, compte tenu de son incidence considérable sur le commerce et des différences entre la LPRPDE et le RGPD[276]. Il a rappelé que le RGPD exigera un examen des décisions concernant le caractère adéquat tous les quatre ans et que la décision, qui permet depuis 2001 le transfert de données de l'UE vers le Canada, devra être revue[277]. Le commissaire a également cité une communication de la Commission européenne de janvier 2017, selon laquelle :

> le caractère adéquat du Canada est "partiel", c'est-à-dire qu'il s'applique uniquement à la LPRPDE, et que toutes les décisions à venir concernant le caractère adéquat reposeront sur une évaluation exhaustive du régime de protection de la vie privée du pays. Cette évaluation portera notamment sur l'accès des autorités publiques aux données personnelles aux fins d'application de la loi, de sécurité nationale et d'autres objectifs d'intérêt public[278].

Pour sa part, M^me^ Campbell, d'Innovation, Sciences et Développement économique Canada, a invité le gouvernement à entamer la discussion sur l'examen du caractère adéquat de la LPRPDE avec les représentants de la Commission européenne[279]. Cependant, selon M^me^ Campbell,

> Notre régime de protection de la vie privée doit continuer d'évoluer indépendamment des mesures prises par la Commission européenne, tout simplement parce que l'Internet des objets arrive à grands pas. Le consentement des enfants est un enjeu crucial à l'échelle nationale et internationale. Nous devons nous assurer que notre

275 ETHI, Mémoire du Commissaire à la protection de la vie privée du Canada, 2 décembre 2016.

276 ETHI, *Témoignages*, 1re session, 42e législature, 16 février 2017, 1540 (Daniel Therrien).

277 *Ibid*.

278 *Ibid*.

279 ETHI, *Témoignages*, 1re session, 42e législature, 9 mai 2017, 1650 (Krista Campbell).

> régime évolue pour s'adapter aux changements technologiques et aux défis auxquels nous faisons face – et non juste parce que les Européens le font[280].

Dans le même ordre d'idées, M^me^ Reynolds, de chez Torys LLP, a suggéré au Comité de

> [ne] pas se focaliser sur des réformes qui consisteraient simplement à adopter les décisions de l'Union européenne en matière d'adéquation, mais bien plutôt sur une harmonisation entre la loi canadienne et les normes internationales de manière à assurer une meilleure protection des renseignements des consommateurs et des entreprises et à accroître la prévisibilité sur l'ensemble des territoires[281].

M. Buttarelli, le contrôleur européen de la protection des données, a expliqué qu'il voit « une continuité entre la législation actuelle et la législation future pour donner un sens aux droits et libertés existants et nouveaux pour les gens ordinaires et pour en accroître l'efficacité dans la pratique[282] ». Il a d'ailleurs rappelé que toutes les décisions d'adéquation existantes demeureront en vigueur jusqu'à ce qu'elles soient mises à jour ou abrogées[283]. Selon M. Buttarelli, l'UE n'est pas pressée « de mettre le Canada au haut de nos priorités pour les décisions. Vous devriez maintenant vérifier ce qu'il faut, au regard de la nouvelle liste détaillée de critères figurant désormais dans le RGPD pour l'évaluation de cette adéquation[284] ».

M. Buttarelli a rappelé qu'en vertu de la décision *Schrems* de la CJUE, le critère à utiliser désormais pour déterminer ce qui est adéquat est « essentiellement l'équivalent[285] ». Dans leur recherche de l'adéquation de la LPRPDE au RGPD, il a recommandé aux membres du Comité

> de ne pas vous attarder outre mesure aux nouveautés dans le RGPD, comme le principe de protection des données dès la conception, le principe de protection des données par défaut, et le principe de la transférabilité […] Nous vous encourageons à privilégier une approche globale et non à reprendre chacune des règles, point par point […] les restrictions, les exceptions et les dérogations à l'application de la loi sont plus importantes que les principes à dessein et par défaut[286].

---

280 *Ibid*., 1645.

281 ETHI, *Témoignages*, 1re session, 42e législature, 6 avril 2017, 1625 (Molly Reynolds).

282 ETHI, *Témoignages*, 1re session, 42e législature, 13 juin 2017, 1210 (Giovanni Buttarelli).

283 *Ibid*.

284 *Ibid*.

285 *Ibid*., 1215.

286 *Ibid*., 1245 et 1250.

En somme, selon M. Buttarelli, c'est l'application de la loi qui est au sommet des préoccupations européennes[287].

Certains témoins ont fait valoir que des modifications devraient être apportées à la LPRPDE dès maintenant dans le but de tendre vers l'adéquation avec le RGPD[288].

Pour sa part, M[me] Stoddart a invité le Comité à placer la barre haut au moment d'envisager la modernisation de la LPRPDE et de se rappeler que le RGPD applique aussi les normes européennes à l'utilisation des renseignements personnels dans le secteur public[289]. Elle a souligné le problème qui découle du fait que les critères de l'adéquation, qui sont plus rigoureux que ceux prévus dans la LPRPDE, ne sont pas définis de façon précise dans le RGDP[290]. Selon M[me] Stoddart,

> Le problème le plus grave, c'est qu'au sein de l'Union européenne, selon mon étude de toutes les décisions où il a été déterminé que le niveau de protection était adéquat ou qui ont donné lieu à une analyse, l'historique d'évaluation des cadres de protection des renseignements personnels est très inégal d'un pays à l'autre[291].

Mme Stoddart a également souligné que ce problème s'ajoute au fait qu'il existe des pressions au sein de l'UE pour que les normes européennes soient imposées avec rigueur au reste du monde[292].

Dans une perspective d'échanges commerciaux entre le Canada et l'UE, M[e] Bernier a recommandé que le Canada ait déjà renforcé ses mesures de protection de la vie privée à un niveau acceptable pour l'UE au moment où cette dernière déterminera le caractère adéquat de la législation canadienne[293].

M. Martin-Bariteau a souligné qu'il convient de mettre à jour le droit canadien pour passer le test d'adéquation du RGPD, tout en gardant en tête que ce test ne demande pas une copie carbone du RGPD et qu'il concerne tous les régimes de protection de la

---

287 *Ibid*., 1250.

288 ETHI, *Témoignages*, 1re session, 42e législature, 21 février 2017, 1530 (Drew McArthur); ETHI, *Témoignages*, 1re session, 42e législature, 21 février 2017, 1540 (Jill Clayton, commissaire, Bureau du Commissaire à l'information et à la protection de la vie privée de l'Alberta); ETHI, *Témoignages*, 1re session, 42e législature, 16 mai 2017, 1600 (Dennis Hogarth).

289 ETHI, *Témoignages*, 1re session, 42e législature, 23 mars 2017, 1620 (Jennifer Stoddart).

290 *Ibid*.

291 *Ibid*.

292 *Ibid*.

293 ETHI, *Témoignages*, 1re session, 42e législature, 14 février 2017, 1650 (Chantal Bernier).

vie privée, pas seulement la LPRPDE[294]. Selon lui, certaines modifications à la LPRPDE seraient nécessaires, mais suffisantes, pour une adéquation au RGPD, comme le fait d'encadrer plus strictement la rétention par les organisations des données dans le temps et d'accorder un droit direct aux justiciables[295].

D'autres témoins ont invité le Comité à faire preuve de patience et ont plaidé qu'il serait prématuré de modifier la LPRPDE maintenant[296].

M. Bennett, de l'Université de Victoria, a pour sa part suggéré de moderniser la LPRPDE parce qu'elle a besoin d'être mise à jour et non dans le seul but de respecter les exigences relatives au caractère adéquat prévues dans le RGDP, qui sont très vagues, selon lui[297]. Il a cependant identifié trois secteurs où les divergences entre la LPRPDE et le RGDP seraient les plus flagrantes : les pouvoirs d'application de la loi du commissaire; le fait que le commissaire dispose de tous les outils disponibles en matière de protection des renseignements personnels; et le traitement des données sensibles[298].

2. L'importance de l'application de la loi dans l'évaluation du caractère adéquat

En ce qui a trait au volet de l'application de la *Loi*, M^me^ Scassa a argué que le manque de pouvoirs d'exécution du commissaire à la protection de la vie privée représente également la plus grande faiblesse de la LPRPDE par rapport à sa conformité aux normes européennes, ce qui rejoint le point de vue européen exprimé par M. Buttarelli et cité précédemment[299].

Dans le même ordre d'idées, M. Israel, de la CIPPIC, a argué que la question de l'application de la loi pourrait poser problème dans la détermination du caractère adéquat de la LPRPDE par rapport au RGDP. En effet, il considère que « c'est un volet dans lequel nous sommes en décalage par rapport à d'autres commissariats à la protection des données dans le monde, et que l'Union européenne a amélioré les choses de façon considérable sur ce plan récemment[300] ».

---

294 ETHI, *Témoignages*, 1re session, 42e législature, 23 février 2017, 1550 (Florian Martin-Bariteau).

295 *Ibid*., 1620.

296 ETHI, *Témoignages*, 1re session, 42e législature, 23 mars 2017, 1645 (Suzanne Morin), ETHI, *Témoignages*, 1re session, 42e législature, 4 avril 2017, 1615 (David Young); ETHI, *Témoignages*, 1re session, 42e législature, 11 mai 2017, 1645 (Wally Hill); ETHI, *Témoignages*, 1re session, 42e législature, 30 mai 2017, 1605 (Adam Kardash).

297 ETHI, *Témoignages*, 1re session, 42e législature, 21 mars 2017, 1640 (Colin Bennett).

298 *Ibid*., 1640 et 1645.

299 ETHI, *Témoignages*, 1re session, 42e législature, 23 février 2017, 1620 (Teresa Scassa).

300 ETHI, *Témoignages*, 1re session, 42e législature, 23 mars 2017, 1705 (Tamir Israel).

3. Le consentement des enfants dans le *Règlement général sur la protection des données*

M. Charters, de RJC, a recommandé de suivre l'exemple de l'UE qui exige dans le nouveau RGPD le consentement d'un parent ou d'un tuteur pour accéder à des services en ligne pour les enfants de moins de 16 ans (ou moins, pour autant que l'âge prévu soit d'au moins 13 ans)[301]. Selon lui,

> il importe que les parents soient présents, parce qu'eux seulement devraient être en mesure de fournir un consentement éclairé et explicite en échange de la collecte de renseignements. Les parents devraient être informés et responsables des activités de leurs enfants en ligne. Les mécanismes qui imposent un consentement parental explicite servent également à assurer la participation et la vigilance en regard de ce que les enfants visitent et explorent en ligne[302].

Le Comité se rend aux arguments des témoins qui ont suggéré d'entreprendre sans tarder des démarches pour que la législation canadienne tende vers l'adéquation au RGPD, tout en reconnaissant que la LPRPDE n'est qu'un élément de la législation concernée et que cette adéquation doit être atteinte en conservant la spécificité canadienne. Pour ces raisons, le Comité recommande :

Recommandation 17 sur les critères d'adéquation entre la *Loi sur la protection des renseignements personnels et les documents électroniques* et le *Règlement général sur la protection des données* :

Que le gouvernement du Canada collabore avec les autorités de l'Union européenne afin de déterminer quels seraient les critères requis pour que la *Loi sur la protection des renseignements personnels et les documents électroniques* soit considérée comme adéquate au regard du *Règlement général sur la protection des données*.

Recommandation 18 sur les modifications législatives requises pour conserver le caractère adéquat :

a) **Que le gouvernement du Canada identifie quelles seraient les modifications à apporter à la *Loi sur la protection des renseignements personnels et les documents électroniques*, s'il y a lieu, afin qu'elle conserve son caractère adéquat au regard du *Règlement général sur la protection des données*; et**

301 ETHI, *Témoignages*, 1re session, 42e législature, 25 septembre 2017, 1540 (Owen Charters).

302 *Ibid*.

b) Que, dans l'éventualité où il serait déterminé que les modifications requises pour conserver le caractère adéquat ne sont pas dans l'intérêt du Canada, le gouvernement du Canada crée des mécanismes permettant un échange de données sans heurts entre le Canada et l'Union européenne.

Recommandation 19 sur la collaboration avec les provinces et territoires :

Que le gouvernement du Canada collabore avec les provinces et les territoires pour s'assurer que tous les ordres de gouvernement concernés sont au fait des exigences relatives à la reconnaissance du caractère adéquat par les autorités de l'Union européenne.

MISSION DU COMITÉ À WASHINGTON (D.C.), DU 2 AU 4 OCTOBRE 2017

Du 2 au 4 octobre 2017, quatre membres du Comité se sont rendus à Washington dans le cadre de l'étude sur la LPRPDE. L'objectif général de cette mission était d'obtenir une meilleure compréhension des lois et du cadre des États-Unis en matière de protection de la vie privée, dans une perspective comparative. Les membres du Comité ont rencontré divers intervenants qui les ont informés des enjeux relatifs à la protection de la vie privée aux É.-U. Il a principalement été question des pouvoirs d'application de la loi, de la protection des renseignements personnels, de la législation basée sur des principes, ainsi que de la notion de consentement et de transparence algorithmique.

A. Cadre législatif des États-Unis en matière de protection de la vie privée et aperçu de la Federal Trade Commission

1. Cadre américain

Il importe avant toute chose de souligner que les É.-U. n'ont pas de cadre national complet pour la protection de la vie privée. En fait, les É.-U. n'ont pas adopté de loi générale sur la protection de la vie privée. Il existe, au niveau du gouvernement fédéral et dans les États, divers lois et règlements régissant la protection de la vie privée. Ainsi, les mesures de protection de la vie privée varient d'un État à l'autre.

Par exemple, la Californie a adopté un cadre législatif rigoureux relatif à la protection de la vie privée[303]. Le cadre législatif de la Californie inclut une Constitution qui « garantit à

303 Tony Cárdenas, député démocrate du 29e district de la Californie au Congrès, membre du Subcommittee on Digital Commerce and Consumer Protection.

chaque citoyen le “droit inaliénable” à la protection de la vie privée[304] » et une série de lois régissant divers secteurs. Tony Cárdenas[305], membre du Subcommittee on Digital Commerce and Consumer Protection du Committee on Energy and Commerce de la Chambre des représentants des É.-U., ainsi que des chercheurs du service de recherche du Congrès, ont indiqué que la Californie est l’un des États les plus stricts en matière de protection de la vie privée.

En conséquence, il n’existe aux É.-U. aucune loi équivalente à la LPRPDE. Des représentants de la Federal Trade Commission (FTC)[306] et du Center for Democracy and Technology (CDT)[307] ont indiqué que le « Wild West » règne actuellement dans le domaine de la réglementation de la protection de la vie privée aux É.-U., et que de meilleurs outils de protection de la vie privée et des moyens de dissuasion doivent être mis en place. Des chercheurs du service de recherche du Congrès ont indiqué que, aux É.-U., la protection de la vie privée semble très importante en ce qui concerne les activités du gouvernement. Toutefois, la question de la protection de la vie privée inquiète moins les citoyens américains lorsqu’il s’agit des entreprises.

2. La Federal Trade Commission

La FTC, dont le siège est à Washington, est un organisme fédéral bipartite[308] ayant la double mission de protéger les consommateurs et de promouvoir la concurrence[309]. Au sein de la FTC, le Bureau of Consumer Protection est chargé de réprimer les pratiques commerciales inéquitables, trompeuses et frauduleuses[310]. L’organisme compte parmi

304 États-Unis (É.-U.), département de la Justice de la Californie, *Privacy Laws*.

305 É.-U., Tony Cárdenas, membre du Congrès, *Biography*.

306 Représentants de la FTC :

- Tom Pahl, directeur par intérim du Bureau of Consumer Protection
- Kathleen Benway, directrice du bureau de Tom Pahl
- Maneesha Mithal, directrice associée, Division of Privacy and Identity Protection
- Stacy Feuer, directrice adjointe, Office of International Affairs
- Guilherme Roschke, conseiller, International Consumer Protection

307 É.-U., Center for Democracy and Technology [CDT], *About CDT*; représentants : Chris Calabrese, vice-président, Policy, et Michelle de Mooy, directrice, Privacy and Data Project.

308 La FTC est dirigée par cinq commissaires, nommés par le Président. Leur nomination doit être entérinée par le Sénat. Le mandat des commissaires est d’une durée de sept ans. Au maximum trois commissaires peuvent appartenir au même parti politique. Voir FTC, Commissaires.

309 É.-U., Federal Trade Commission [FTC], *What We Do*.

310 FTC, *About the Bureau of Consumer Protection*.

ses divisions la Division of Privacy and Identity Protection[311]. Cette division supervise entre autres les questions liées à la protection de la vie privée et des renseignements personnels des consommateurs[312].

Les représentants de la FTC ont expliqué aux membres du Comité que la FTC est le principal agent d'application de la loi au niveau fédéral en ce qui concerne la protection de la vie privée, bien qu'il n'existe aucun régime complet à cet égard. Par exemple, la FTC reçoit les plaintes en matière de sécurité des données.

Essentiellement, la FTC est chargée d'appliquer la *Federal Trade Commission Act* (la « *FTC Act* »)[313]. En général, la compétence de la FTC en ce qui concerne la protection des renseignements personnels et de la vie privée découle de l'article 5 de la *FTC Act*, qui interdit les méthodes, les activités ou les pratiques commerciales inéquitables et trompeuses[314]. Il convient de noter que les pratiques « inéquitables » sont définies comme celles « qui causent, ou risquent de causer au consommateur un préjudice que ce dernier ne peut lui-même raisonnablement éviter et qui n'est pas contrebalancé par des avantages compensateurs pour le consommateur ou la concurrence[315] ».

La FTC est aussi chargée d'appliquer des lois propres à certains secteurs, telles que la *Children's Online Privacy Protection Rule* (COPPA), qui « impose certaines exigences aux exploitants de sites Web ou de services en ligne destinés aux enfants de moins de 13 ans[316], la *Safeguards Rule*, qui « exige des institutions financières relevant de la FTC qu'elles mettent en place des mesures assurant la protection des renseignements des clients[317] » et la *Fair Credit Reporting Act*, laquelle « assure la protection des renseignements recueillis par les agences de renseignements sur les consommateurs comme les agences d'évaluation du crédit, les entreprises de renseignements médicaux et les services de présélection de locataires[318].

Les représentants de la FTC ont indiqué que leur intervention se fait essentiellement en aval, mais que l'organisme a tenté de publier plus de documentation informant les

311 *Ibid*.

312 *Ibid*.

313 É.-U., 15 U.S.C. §§ 41-58, article 5.

314 *Ibid*.

315 É.-U., FTC, *A Brief Overview of the Federal Trade Commission's Investigative and Law Enforcement Authority*.

316 É.-U., *Children's Online Privacy Protection Rule ("COPPA")*, 16 CFR partie 312.

317 É.-U., *Safeguards Rule*, 16 CFR partie 314.

318 É.-U., FTC, *Fair Credit Reporting Act*, 15 U.S.C. §§ 1681-1681x.

entreprises sur ce qu'elles doivent faire pour se conformer à la loi. La FTC a donc mis davantage l'accent sur les conseils aux entreprises.

B. Pouvoirs d'exécution

Au cours de leur mission, les membres du Comité ont discuté avec les intervenants des pouvoirs du commissaire à la protection de la vie privée du Canada par rapport à ceux de la FTC.

1. Pouvoirs d'exécution de la Federal Trade Commission

La FTC a renvoyé les membres du Comité au mémoire que l'organisme a présenté au CPVP du Canada dans le cadre des consultations du Commissariat sur la protection de la vie privée et le consentement. Dans son mémoire, la FTC recommande de renforcer les pouvoirs du commissaire à la protection de la vie privée du Canada[319].

Les représentants de la FTC ont expliqué que la *FTC Act* donne des pouvoirs d'exécution à la FTC, tels que le pouvoir d'émettre des ordonnances et d'exercer des recours pour les consommateurs dans certains cas.

Au sujet des ordonnances, la FTC soulignait dans son mémoire au Commissariat qu'elle :

> peut obtenir, dans ses procédures devant les tribunaux administratifs ou les cours fédérales, des ordonnances juridiquement exécutoires, dans le cadre d'un règlement (ordonnance par consentement) ou d'une poursuite judiciaire. Le pouvoir qu'a l'organisme de demander des ordonnances est la pierre angulaire de son rigoureux programme d'application de la loi et constitue une mesure efficace d'incitation à la conformité pour les entreprises. En effet, le pouvoir de délivrer ou de demander de telles ordonnances est conforme aux pratiques exemplaires internationales établies dans les lignes directrices sur la protection de la vie privée de l'OCDE, qui appellent les pays membres à veiller à ce que leurs responsables de la protection du droit à la vie privée aient la capacité de prévenir et sanctionner la violation des lois nationales à cet égard et puissent prendre des mesures correctives contre les entreprises dont les pratiques contreviennent à ces lois.
>
> Le pouvoir de la FTC d'émettre des ordonnances découle de la *FTC Act*, laquelle autorise l'organisme à faire appliquer la loi par les voies administratives et judiciaires. Dans le cadre du processus administratif, l'organisme, après une enquête et un règlement ou une décision administrative, peut émettre une ordonnance prescrivant des pratiques précises et imposant des exigences pour assurer la conformité ultérieure du défendeur. Dans le cadre du processus judiciaire, la FTC peut demander une injonction provisoire

319 CPVP, *Mémoire reçu dans le cadre de la consultation sur le consentement en vertu de la LPRPDE (FTC)*.

> ou permanente auprès d'une cour fédérale afin de faire appliquer toute disposition de la loi dont l'exécution relève de la Federal Trade Commission.
>
> […]
>
> Les ordonnances administratives et judiciaires obtenues par la FTC peuvent comprendre plusieurs dispositions d'injonction fondamentales, selon les circonstances de la mesure d'exécution en question. Parmi celles-ci : (1) l'interdiction de s'adonner à l'activité contestée, ou à une activité semblable, à l'avenir; (2) selon le cas, l'obligation de mettre en place un programme complet de protection de la vie privée ou des données, conformément aux précisions de l'ordonnance; (3) l'adoption de mesures de contrôle et de conformité concrètes pour une période déterminée (p. ex., obligation de conserver des dossiers d'entreprise, d'informer les employés de l'ordonnance ou d'aviser la Commission de tous changements pouvant avoir un effet sur le respect des obligations). Les exigences sur les mesures concrètes permettent à la FTC de mieux contrôler le respect de l'ordonnance de la *FTC Act*[320].

Les représentants de la FTC ont également informé les membres du Comité que l'organisme a mis en œuvre des mesures d'exécution touchant un grand nombre de questions reliées à la protection de la vie privée, tels que les pourriels, les espiogiciels, le réseautage social, etc.[321]. La FTC a indiqué que ces questions reliées à la protection de la vie privée comprenaient plus de 130 cas de pourriels et d'espiogiciels et plus de 40 poursuites en matière de protection de la vie privée en général[322]. Les représentants de la FTC ont aussi mentionné que, depuis 2002, l'organisme « a intenté plus de 60 recours contre des entreprises ayant utilisé des pratiques inéquitables ou trompeuses qui ont exposé les renseignements personnels des consommateurs à un risque déraisonnable[323] ». L'organisme a précisé que, lorsqu'elle juge qu'une entreprise n'a pas correctement protégé les données, la FTC exige habituellement que l'entreprise mette en place un programme complet de protection des renseignements, autrement dit un plan de protection, assujetti à des évaluations et des vérifications. Les représentants de la FTC ont indiqué que Facebook et Google font l'objet d'une ordonnance de la FTC, ce qui signifie qu'elles sont sous haute surveillance. Les représentants ont résumé les dossiers et indiqué que ceux-ci ont été rendus publics. Voici les conclusions des enquêtes et des ententes négociées pour Google et Facebook :

- **Google** : En 2010, l'entreprise a lancé Google Buzz, un nouveau réseau social offert dans l'application Gmail. En résumé, « bien que Google ait

320 *Ibid*. [TRADUCTION]

321 É.-U., FTC, *Privacy & Data Security- Update: 2016*.

322 *Ibid*.

323 *Ibid*.

laissé croire aux utilisateurs de Gmail qu'ils étaient libres d'accepter ou de refuser d'adhérer au réseau, les options permettant de refuser d'adhérer au réseau ou de s'en retirer étaient inopérantes[324] ». La situation a donné lieu à une plainte auprès de la FTC. En mars 2011, la FTC a annoncé que Google avait accepté de

> négocier un règlement concernant les accusations de la Federal Trade Commission, selon lesquelles l'entreprise avait employé des tactiques trompeuses et violé ses propres engagements en matière de protection de la vie privée pris envers les consommateurs lorsqu'elle a lancé son réseau social Google Buzz, en 2010. L'organisme prétend que ces pratiques contreviennent à la *FTC Act*. Le projet de règlement [en anglais seulement] interdit à l'entreprise toute fausse déclaration future en matière de protection de la vie privée, l'oblige à mettre en place un programme complet de protection de la vie privée et demande l'exécution régulière de vérifications indépendantes en matière de protection de la vie privée pour les 20 prochaines années[325].

- **Facebook** : En 2011, la FTC a annoncé que Facebook avait accepté de « négocier un règlement concernant les accusations de la Federal Trade Commission, selon lesquelles l'entreprise avait trompé les consommateurs en leur disant qu'ils pouvaient assurer la confidentialité de leurs renseignements dans Facebook, avant d'en permettre à maintes reprises la communication et la publication[326] ».

  > Le projet de règlement interdit à Facebook de faire toute autre déclaration trompeuse de confidentialité, exige que l'entreprise obtienne l'approbation des consommateurs avant de modifier la façon dont elle communique leurs renseignements, et l'oblige à faire évaluer périodiquement ses pratiques de protection de la vie privée par des vérificateurs indépendants pour les 20 prochaines années[327].

Enfin, les représentants de la FTC ont abordé la question de leur pouvoir de demander l'imposition de pénalités financières. Dans son mémoire, la FTC donne à cet égard les précisions suivantes :

> La FTC demande couramment l'imposition de pénalités financières dans les cas de fraude à la consommation et de publicité trompeuse, à la fois pour réparer les préjudices financiers subis par les consommateurs et pour priver les accusés de gains

---

324 É.-U., FTC, *FTC Charges Deceptive Privacy Practices in Googles Rollout of Its Buzz Social Network*, « Google Agrees to Implement Comprehensive Privacy Program to Protect Consumer Data », 30 mars 2011.

325 *Ibid*.

326 É.-U., FTC, *Facebook Settles FTC Charges That It Deceived Consumers By Failing To Keep Privacy Promises*.

327 *Ibid*.

> financiers illégitimes. Ce pouvoir d'imposer des pénalités financières découle de trois sources juridiques. Premièrement, la *FTC Act* autorise la FTC à déposer des poursuites devant des cours de district fédéral afin d'obtenir des injonctions provisoires ou permanentes à l'égard de pratiques commerciales inéquitables ou trompeuses qui contreviennent à la *FTC Act*. En plus des mesures correctives visant les activités, telles que celles décrites ci-dessus, ces injonctions peuvent comprendre, selon le cas, des réparations pécuniaires équitables pouvant prendre la forme de restitutions aux consommateurs et de remises de profits. Deuxièmement, la FTC est habilitée à demander des sanctions civiles dans les cas de violations d'ordonnances administratives. Troisièmement, la FTC a le pouvoir d'imposer des sanctions civiles pécuniaires lorsque de telles sanctions sont expressément prévues par une loi, selon les montants maximums fixés par la loi[328].

Il convient de noter que les représentants de la FTC ont souligné qu'un préjudice substantiel doit être prouvé afin d'obtenir réparation en vertu de la *FTC Act*. Ils ont toutefois indiqué qu'il est difficile de caractériser les préjudices que subissent les consommateurs dans les cas d'incidents liés à la sécurité des données et que l'on ne sait pas très bien comment mesurer les préjudices. Les représentants de la FTC ont fait remarquer qu'ils allaient bientôt tenir une conférence sur la question[329].

2. Les pouvoirs du commissaire à la protection de la vie privée du Canada

i) Le point de vue de la Federal Trade Commission

Les représentants de la FTC ont insisté sur le fait que, selon eux, le commissaire à la protection de la vie privée du Canada devait avoir plus de pouvoirs exécutoires aux fins d'application de la loi et ont de nouveau renvoyé les membres du Comité au mémoire de la FTC au CPVP.

Premièrement, dans son mémoire, la FTC précisait que « le Commissariat pourrait mieux protéger la vie privée […] en se livrant à des activités proactives d'application de la loi – plutôt qu'en répondant uniquement aux plaintes[330] ». La FTC a expliqué que, d'après son expérience :

> Les plaintes ne constituent pas une source d'information suffisante pour permettre aux autorités de faire enquête sur les nouvelles questions liées à la protection de la vie privée et de donner suite à celles qui suscitent le plus d'inquiétudes sur le plan de la protection de la vie privée. Cette situation est en grande partie liée à l'ampleur du volume de données personnelles généré et au fait que les systèmes complexes utilisés

328 *Ibid*.

329 La FTC a tenu un atelier d'information sur les préjudices le 12 décembre 2017, voir FTC, *Informational Injury Workshop*.

330 CPVP, *Mémoire reçu dans le cadre de la consultation sur le consentement en vertu de la LPRPDE (FTC)*.

> pour la collecte des données rendent souvent la tâche difficile, voire impossible, aux consommateurs quand il s'agit de cerner les atteintes à la vie privée et de présenter des plaintes à cet égard. Les autorités d'application de la loi ont avantage à utiliser diverses sources d'information – y compris les nouveaux rapports, les recherches internes et universitaires réalisées par les spécialistes de la protection de la vie privée et de la sécurité, les renvois du Congrès, les divulgations des entreprises et des concurrents, ainsi que les renseignements des organismes partenaires d'application de la loi nationaux et internationaux – afin de cerner les menaces à la vie privée et d'établir leurs priorités en matière d'application de la loi[331].

Deuxièmement, dans son mémoire, la FTC a affirmé que si le CPVP avait le pouvoir d'émettre des ordonnances, il pourrait mieux protéger la vie privée. La FTC a indiqué que « les ordonnances fournissent non seulement un fondement de grande valeur pour la surveillance de la conformité et l'application de la loi par la FTC, mais elles peuvent procurer un avantage accru en communiquant les attentes de la FTC aux entreprises de façon plus générale[332] ».

Troisièmement, dans son mémoire, la FTC insiste sur le fait que, à son avis, si le CPVP avait le pourvoir d'imposer des pénalités financières, il pourrait mieux protéger la vie privée. La FTC a expliqué que « la capacité d'imposer des pénalités financières, que ce soit sous la forme d'amendes réglementaires ou de mesures de redressement équitables comme le remboursement et la restitution (dans les cas où les consommateurs subissent des pertes financières), peut servir d'outil important pour promouvoir la conformité et décourager tout comportement illégal[333] ».

ii) Le point de vue de Facebook

Les représentants de Facebook[334] ont insisté sur le fait qu'ils consultent constamment le CPVP et qu'ils l'ont consulté plusieurs fois dans le passé. Ils ont indiqué que le régime de la LPRPDE permet une approche collaborative, une approche qu'ils jugent efficace. Ils ont ajouté qu'en donnant au commissaire à la protection de la vie privée plus de pouvoirs, comme le pouvoir d'ordonnance, on changerait la relation entre les entreprises et le CPVP. Ils ont aussi souligné que les pouvoirs proactifs, tels que le pouvoir de mener des vérifications et d'émettre des ordonnances, peuvent entraîner des coûts pour les entreprises. Ils ont indiqué que l'approche collaborative que permet

331 *Ibid*.

332 *Ibid*.

333 *Ibid*.

334 Représentants : Rob Sherman, dirigeant principal adjoint de la protection de la vie privée, Claire Gartland, gestionnaire, Vie privé et politiques publiques et Kevin Chan, chef, Politiques publiques, Canada.

la LPRPDE au Canada constitue une importante considération et un facteur positif dont les entreprises tiennent compte lorsqu'elles déterminent où investir.

C. La protection des renseignements personnels et l'atteinte à la protection des données d'Equifax

Dans le cours de leurs activités et dans une industrie axée sur les données, les entreprises recueillent des renseignements personnels des consommateurs. Les mesures de protection des renseignements personnels sont importantes car les atteintes aux renseignements personnels peuvent causer des préjudices aux consommateurs, tel qu'il a été constaté avec la récente atteinte à la protection des données d'Equifax. Cependant, les intervenants ont indiqué qu'il est difficile d'atteindre le juste équilibre entre l'innovation, la croissance économique et la réglementation.

1. Atteinte à la protection des données d'Equifax

Le 3 octobre 2017, le Subcommittee on Digital Commerce and Consumer Protection du Committee on Energy and Commerce de la Chambre des représentants des États-Unis a tenu une audience intitulée « Oversight of the Equifax Data Breach : Answers for Consumers » durant laquelle l'ancien PDG d'Equifax a témoigné au sujet de l'atteinte à la protection des données[335]. Les membres du Comité à Washington ont assisté à cette réunion.

i) Contexte

Equifax est une entreprise d'analyse et de rapport de crédit dont le siège social se situe à Atlanta en Géorgie. « La société structure, assimile et analyse les données de plus de 820 millions de consommateurs et de plus de 91 millions d'entreprises dans le monde et ses bases de données comprennent les données d'employés fournies par plus de 7 100 employeurs[336]. » L'entreprise « compte quelque 9 900 employés à travers le monde[337] ». Elle « a des investissements ou des exploitations dans 24 pays en Amérique du Nord, en Amérique centrale, en Amérique du Sud, en Europe et dans la région Asie-Pacifique. Elle est membre de l'indice Standard & Poor's (S&P) 500®. Les actions

335 Committee on Energy and Commerce, *Oversight of the Equifax Data Breach: Answers for Consumers*, 3 octobre 2017.

336 Equifax, *Profil de l'entreprise*.

337 *Ibid*.

ordinaires de l'entreprise se négocient à la Bourse de New York sous le symbole EFX[338] ».

Le 7 septembre 2017, Equifax a « annoncé que des criminels avaient exploité la vulnérabilité d'une application du site Web aux É.-U. afin d'obtenir un accès à certains dossiers[339] » et que « selon l'enquête menée par l'entreprise, les accès non autorisés se sont produits de la mi-mai jusqu'à juillet 2017[340] ». Aux États-Unis, l'incident a touché potentiellement les renseignements personnels de 143 millions de clients américains[341]. Les représentants d'Equifax ont expliqué que « l'incident touche potentiellement l'information personnelle d'environ 100 000 consommateurs canadiens et que l'information en cause pourrait comprendre le nom, l'adresse, le numéro d'assurance sociale et, dans des cas limités, les numéros des cartes de crédit[342] ».

Le 26 septembre 2017, Equifax a annoncé que Richard Smith quittait ses fonctions de président du conseil et directeur général (PDG) d'Equifax[343].

Le 2 octobre 2017, Equifax Canada a déclaré qu'environ 8 000 Canadiens ont été touchés par l'atteinte à la protection des données, révisant ainsi à la baisse son estimation précédente à l'effet que 100 000 Canadiens auraient pu être touchés[344]. Equifax Canada a également révélé qu'elle avait pris connaissance de l'incident le 29 juillet 2017[345].

Le 28 novembre 2017, Equifax Canada a révisé à la hausse son estimation du nombre de Canadiens touchés par l'atteinte à la protection des données qu'elle a subie[346]. En effet, Equifax a révélé que les cartes de crédit de 11 670 Canadiens avaient été piratées, ce qui ferait passer le total de clients affectés de 8 000 à environ 19 000. Equifax a également

338 *Ibid*.

339 Equifax, Bulletins de presse, *Equifax donne aux Canadiens des éclaircissements supplémentaires sur l'incident de cybersécurité impliquant de l'information de consommateurs*, 19 septembre 2017.

340 *Ibid*.

341 Equifax, *Equifax Releases Details on Cybersecurity Incident, Announces Personnel Changes*.

342 Equifax, Bulletins de pesse, *Equifax donne aux Canadiens des éclaircissements supplémentaires sur l'incident de cybersécurité impliquant de l'information de consommateurs*, 19 septembre 2017.

343 Equifax, *Equifax Chairman, CEO, Richard Smith Retires; Board of Directors Appoints Current Board Member Mark Feidler Chairman; Paulino do Rego Barros, Jr. Appointed Interim CEO; Company to Initiate CEO Search*.

344 Equifax, *Incident de cybersécurité & Importante information pour les consommateurs*.

345 *Ibid*.

346 La Presse canadienne, *Equifax : plus de 19 000 Canadiens ont été touchés par la cyberattaque*, *LaPresse.ca*, 28 novembre 2017.

confirmé que son enquête a conclu que les dossiers de carte de crédit piratés contenaient les noms, adresses, numéros de carte de crédit et de débit (et leurs dates d'expiration) des clients concernés, en plus de leurs numéros d'assurance sociale. Equifax Canada a indiqué que les systèmes informatiques canadiens n'ont pas été touchés et qu'ils sont « entièrement séparés » des systèmes en place aux États-Unis[347].

Le personnel du Energy and Commerce Committee de la Chambre des représentants ont remis aux membres du Comité une note d'information expliquant les exigences du droit américain qui s'appliquent à Equifax en matière de protection de la vie privée[348].

ii) L'audience

L'audience tenue par le Subcommittee on Digital Commerce and Consumer Protection du Committee on Energy and Commerce de la Chambre des représentants des États-Unis avait pour but d'aider les consommateurs à comprendre les mesures prises par Equifax afin de protéger leurs renseignements personnels à l'avenir, ainsi qu'à aider les individus dont les renseignements personnels ont été touchés. En conséquence, les discussions tenues lors de l'audience ont porté sur la façon dont Equifax a réagi à l'atteinte à la protection des données, la façon dont l'entreprise a corrigé la vulnérabilité dans son système et la façon dont elle a avisé les personnes touchées, entre autres. Des discussions ont aussi été tenues sur l'absence de réglementation dans l'industrie à l'heure actuelle et sur le fait que des mesures de protection de la vie privée doivent être mises en place. On a en outre indiqué que les consommateurs ont besoin des services offerts par les entreprises comme Equifax afin de participer à l'économie : ils n'ont pas d'autres choix.

Dans sa déclaration préliminaire, Bob Latta[349], président du Subcommittee on Digital Commerce and Consumer Protection du Committee on Energy and Commerce de la Chambre des représentants des États-Unis, a dit ceci :

> […] Je parle souvent du fait que nous vivons dans un monde numériquement branché. Ce fait peut avoir de vastes et nombreuses implications positives, pour le commerce, les échanges, les communications et le divertissement. Cette atteinte à la protection des données d'Equifax constitue un cinglant rappel de la présence des acteurs malveillants et des défis de sécurité auxquels est confrontée notre économie numériquement intégrée et alimentée par les données. En l'occurrence, des renseignements personnels de nature délicate utilisés pour constituer les antécédents en matière de crédit et

347 *Ibid*.

348 É.-U., Committee on Energy and Commerce, *Oversight of the Equifax Data Breach: Answers for Consumers*, « Background Memo », 3 octobre 2017.

349 É.-U., Bob Latta, membre du Congrès, *Biography*.

> permettre aux particuliers d'effectuer des opérations commerciales — obtenir des cartes de crédit, acheter des téléphones cellulaires ou des appareils ménagers et contracter des hypothèques — ont été compromis. Des mesures de sécurité raisonnables doivent être mises en place et être appliquées et constamment améliorées par les entreprises qui recueillent et stockent des données, afin de se prémunir contre les accès non autorisés aux renseignements personnels de nature délicate. Autrement, les consommateurs pourraient être exposés à d'importants préjudices financiers[350].

De plus, Jan Schakowsky, membre la plus haut placée de la minorité au Subcommittee on Digital Commerce and Consumer Protection du Committee on Energy and Commerce de la Chambre des représentants, a fait la déclaration suivante lors de l'audience :

> Des agences d'évaluation du crédit, des entreprises à but lucratif non réglementées, recueillent des renseignements personnels et financiers détaillés sur les consommateurs américains. Un véritable trésor pour les pirates. Les consommateurs ne peuvent donner leur avis sur les renseignements qu'Equifax ou, par exemple, TransUnion ou Experian ont recueillis, stockés et vendus. Ce sera souvent une agence d'évaluation du crédit qui déterminera si vous pourrez participer à l'économie moderne d'aujourd'hui, obtenir une carte de crédit, louer un appartement ou même obtenir un emploi. Étant donné que les consommateurs n'ont aucun choix, nous ne pouvons laisser les agences d'évaluation du crédit se réglementer elles-mêmes. On peut choisir de ne pas retourner dans un restaurant où l'on a été malade; on ne peut pas demander à Equifax de ne pas recueillir nos données personnelles[351].

M[me] Schakowsky a ajouté qu'elle et d'autres membres du Commerce and Energy Committee de la Chambre des représentants ont présenté de nouveau un projet de loi qui établirait des normes rigoureuses en matière de sécurité des données, exigerait la publication d'avis en cas d'atteinte à la sécurité des renseignements et prévoirait des mesures d'aide aux victimes d'atteinte à la sécurité des données[352].

2. La protection des renseignements personnels

Au cours de leur mission, les membres du Comité ont discuté avec des intervenants de l'atteinte à la protection des données d'Equifax ainsi que de la protection des renseignements personnels. Les intervenants ont été unanimes à dire que l'atteinte à la protection des données d'Equifax pourrait entraîner d'importants préjudices pour les consommateurs, car les renseignements volés sont de nature hautement délicate et que

350 É.-U., Committee on Energy and Commerce, *Oversight of the Equifax Data Breach: Answers for Consumers*, « Opening Statement of Chairman Bob Latta », 3 octobre 2017.

351 É.-U., Committee on Energy and Commerce, *Oversight of the Equifax Data Breach: Answers for Consumers*, « Unedited Transcripts », 3 octobre 2017.

352 É.-U., Committee on Energy and Commerce, *Oversight of the Equifax Data Breach: Answers for Consumers*, « Unedited Transcripts », 3 octobre 2017.

les effets de l'atteinte aux données pourraient se faire sentir pendant longtemps. En revanche, il n'existait pas de consensus quant aux meilleurs moyens de protéger les renseignements personnels étant donné que la technologie change et évolue. D'une part, certains intervenants préconisent l'introduction dans le droit américain de mesures prescriptives pour la protection des renseignements personnels. D'autre part, certains intervenants ont fait valoir que l'adoption de mesures prescriptives pourrait nuire ou porter préjudice à l'innovation et à la croissance de l'industrie. Par conséquent, des intervenants ont souligné que la question fondamentale est de déterminer comment atteindre un juste équilibre entre la protection de la vie privée, la croissance économique et l'innovation.

Les représentants du CDT et Howard Beales, professeur de gestion stratégique et de politiques publiques à l'Université George Washington[353] ont indiqué qu'il existe des moyens efficaces de protéger les renseignements personnels. M. Beales a ajouté qu'il est impossible d'avoir l'assurance que les mesures de protection fonctionneront toujours et qu'elles protégeront toujours efficacement les renseignements personnels. En fait, les risques changent et l'industrie doit constamment mettre à jour les protections en place. Le CDT a indiqué qu'une approche de protection des renseignements personnels fondée sur des étapes raisonnables serait efficace.

Certains intervenants ont indiqué que, pour favoriser l'innovation et la croissance économique, les entreprises ne devraient pas être réglementées outre mesure. Par exemple, M. Latta, membre du Congrès, a soutenu qu'une réglementation « légère » était le meilleur moyen de régir les entreprises, parce qu'une telle approche leur offre plus de souplesse. M. Harper[354], vice-président du Subcommittee on Digital Commerce and Consumer Protection du Committee on Energy and Commerce de la Chambre des représentants, croit que plus de mesures de protection devraient être exigées afin de protéger les renseignements personnels. Il a indiqué, à titre d'exemple, que les voitures autonomes constituent un important enjeu et que des mesures législatives ont été adoptées par la Chambre des représentants des É.-U. Il a également mentionné que les tests où l'on met les systèmes à l'épreuve et où des tentatives d'hameçonnage sont envoyées aux employés constituent un bon moyen pour assurer la protection de la vie privée. M. Cárdenas, membre du Congrès, est d'avis qu'il devrait y avoir plus de normes prescriptives pour assurer la protection des renseignements personnels des consommateurs. Il a toutefois indiqué que les grandes entreprises sont contre de telles mesures prescriptives. M. Johnson[355], membre du Subcommittee on Communications

353 É.-U., Université George Washington, *Howard Beales*.

354 É.-U., Gregg Harper, membre du Congrès, *Biography*.

355 É.-U., Bill Johnson, membre du Congrès, *Biography*.

and Technology du Committee on Energy and Commerce de la Chambre des représentants, a indiqué qu'il existe un fragile équilibre entre la vie privée et l'industrie. À son avis, l'industrie de la technologie n'a pas été beaucoup réglementée par le passé, raison pour laquelle sa croissance a été si importante et si rapide.

Le personnel de l'Energy and Commerce Committee de la Chambre croit qu'une réglementation « légère » permet une certaine supervision, mais préserve la souplesse de l'industrie. Il convient toutefois que l'atteinte de l'équilibre entre la protection des renseignements personnels, l'innovation et la croissance de l'industrie est une question complexe. Le personnel du comité a aussi mentionné que le département de la Sécurité intérieure met à l'essai des programmes afin de veiller à ce que les entreprises aient des mesures de protection appropriées.

Certains intervenants ont souligné que la protection de la vie privée et l'incidence qu'elle peut avoir sur la réputation des entreprises peuvent encourager ces dernières à mettre en place de rigoureuses mesures de protection de la vie privée. En fait, les atteintes à la protection des renseignements personnels peuvent avoir des conséquences considérables pour les entreprises, qui peuvent perdre la confiance des consommateurs. À titre d'exemple, la FTC a mentionné que, dans la décision d'une entreprise de mettre en place des mesures de protection de la vie privée, sa réputation est une considération importante. M. Johnson, membre du Congrès, a aussi indiqué que les entreprises n'arrivent pas toujours à rétablir leur réputation lorsque celle-ci a été entachée par une atteinte à la protection des données. Les représentants de Facebook ont fait observer que 23 millions de Canadiens utilisent Facebook et que la confiance des consommateurs leur est essentielle. Ils ont dit veiller à ce que les utilisateurs soient informés des questions liées à la protection de la vie privée et à ce qu'ils soient outillés pour prendre des décisions en la matière. Leur vision consiste à faire en sorte que les utilisateurs disposent des renseignements dont ils ont besoin pour vérifier que la « trace » qu'ils laissent dans Internet leur convient.

Enfin, les représentants de la FTC ont fait valoir l'importance des mesures législatives sur les avis en cas d'atteinte à la protection des données. Presque tous les États ont adopté des lois sur les avis d'atteinte à la protection des données, lesquelles exigent que les entités privées et gouvernementales informent les particuliers en cas d'atteinte à la protection des renseignements personnels. Le personnel de l'Energy and Commerce Committee de la Chambre des représentants a indiqué que 48 États, le district de Columbia, Guam, Porto Rico et les Îles Vierges américaines ont établi des exigences sur les avis en cas d'atteinte à la protection des données personnelles.

D. Les principes comme fondement juridique et la notion de consentement

Au cours de leur mission, les membres du Comité ont discuté avec les intervenants de la question des principes comme fondement juridique et de la notion de consentement.

Les représentants de Facebook ont précisé que la LPRPDE, étant fondée sur des principes, est très efficace car elle peut s'adapter à l'évolution technologique. Ils ont dit avoir présenté un mémoire dans le cadre des consultations du CPVP sur la protection de la vie privée et le consentement, dans lequel l'entreprise déclare ceci :

> Facebook est d'avis que, à l'instar du CPVP, l'évolution des technologies, des services, de l'utilisation des données et des modèles opérationnels a bousculé les anciennes façons, plus classiques, d'envisager le consentement et que cette situation persistera sans doute. Nous sommes convaincus que le cadre de la LPRPDE permettra de relever ces défis, mais aussi que le CPVP peut tirer parti de ces mêmes défis pour souligner les forces et la souplesse du régime canadien de protection de la vie privée par rapport à ce qui se fait ailleurs dans le monde.
>
> Nombre des problèmes et inquiétudes peuvent être atténués en utilisant des approches de consentement améliorées, qui sont fondées sur des façons novatrices et conviviales de présenter les pratiques de gestion de renseignements de l'entreprise et qui offrent aux utilisateurs des renseignements clairs sur leurs choix quant à la collecte et à l'utilisation de leurs données, ainsi que sur les façons dont ces choix peuvent être exprimés. Les approches de gouvernance de la protection de la vie privée en ce qui concerne l'élaboration des produits peuvent aussi être fort utiles pour renforcer la responsabilité et améliorer la confiance des consommateurs.
>
> Nous croyons qu'un modèle de protection de la vie privée qui est souple et qui tient compte de diverses approches de consentement adaptées au contexte dans lequel les données sont utilisées constitue encore la meilleure approche afin de permettre aux particuliers de faire des choix quant à leurs renseignements et représente un fondement convenable pour établir un cadre législatif. Il s'agit de l'approche actuellement employée dans la LPRPDE, une loi qui continue de favoriser la confiance et d'encourager la croissance de l'économie numérique[356].

M. Beales s'est déclaré contre un régime de protection de la vie privée fondé sur les principes relatifs à l'équité dans le traitement de l'information[357]. À son avis, un tel régime est trop astreignant pour les consommateurs, parce que les principes mettent

---

356 CPVP, *Consentement et protection de la vie privée : Commentaires de Facebook sur le document de discussion du Commissariat à la protection de la vie privée du Canada*, octobre 2016 [TRADUCTION].

357 Par exemple, les principes relatifs à l'équité dans le traitement de l'information sont des principes que la FTC a mis de l'avant pour la collecte, l'utilisation et la protection des renseignements personnels. La LPRPDE est aussi fondée sur les principes définis dans le Code type sur la protection des renseignements personnels.

habituellement l'accent sur le choix du consommateur. M. Beales a en outre indiqué que l'on constate que des renseignements personnels font l'objet d'une utilisation accessoire qui s'avère être d'une grande valeur, mais que personne n'avait prévu une telle utilisation à l'époque. M. Beales soutient que la solution serait de mettre l'accent sur les risques et les coûts. M. Beales a donc semblé préconiser une approche fondée sur le risque.

Les représentants du CDT ont dit voir d'un bon œil l'approche fondée sur les principes relatifs à l'équité dans le traitement de l'information. Ils ont souligné que la société entre dans une étrange période avec le développement des mégadonnées et de l'Internet des objets[358], par exemple. En conséquence, les représentants du CDT ont indiqué que le moment serait bien choisi pour mettre les principes à jour. De plus, le CDT a souligné l'importance de tenir compte du point de vue des consommateurs. Avec le développement des nouvelles technologies, il est plus difficile pour les consommateurs de comprendre comment les entreprises utilisent leurs renseignements personnels et de distinguer les bons usages des mauvais emplois. En outre, les représentants du CDT ont indiqué que, à l'ère des mégadonnées, le contrôle individuel des renseignements personnels est impossible. La propriété des données ne semble pas être une question dont les entreprises souhaitent discuter ou tenir compte. En revanche, la portabilité des données, telle que le GDPR la prévoit, représente une possibilité, à laquelle l'industrie est plus ouverte.

Les représentants de la FTC ont indiqué qu'une interdiction d'utilisation de renseignements personnels, c'est-à-dire des « zones interdites », serait une très bonne mesure de protection pour les consommateurs. La FTC a soulevé la question de l'opportunité d'une option d'impossibilité de se soustraire à certaines protections à l'égard de certains renseignements personnels.

Les représentants de Facebook ont précisé que leur entreprise utilise l'approche de la protection de la vie privée dès la conception. Ils ont fait observer que la protection de la vie privée est prise en compte sous de nombreux aspects et à une foule d'étapes de l'élaboration des fonctions. Ils ont souligné que le concept de protection de la vie privée dès la conception doit être souple parce qu'il n'a pas la même signification pour les grandes entreprises et les petites entreprises.

Enfin, les chercheurs du service de recherche du Congrès ont indiqué que le droit à l'effacement est une option intéressante, mais qu'elle pourrait être inefficace lorsque les données ont déjà été générées à partir des données qui sont censées être effacées.

358 L'Internet des objets «désigne la mise en réseau d'objets physiques au moyen d'Internet ». Voir Commissaire à la protection de la vie privée du Canada, Internet des objets.

Les représentants de Facebook ont mentionné que, sur sa plateforme, l'entreprise permet aux utilisateurs d'effacer des données qu'ils ont publiées.

E. Transparence algorithmique

Lors de leur mission, les membres du Comité ont tenu des discussions sur la transparence algorithmique. Les algorithmes étant de plus en plus utilisés, notamment pour prendre des décisions, de nombreux intervenants ont attiré l'attention des membres du Comité sur les conséquences éventuelles des algorithmes. Des intervenants ont souligné le fait que les algorithmes peuvent avoir des effets indésirables, comme le ciblage de certains groupes en fonction de la race, de l'origine ethnique ou de considérations socioéconomiques. En conséquence, l'utilisation des algorithmes soulève des questions éthiques.

Le CDT a fait valoir qu'il est très important que les entreprises incorporent les questions d'éthique et de protection de la vie privée au processus de création d'un algorithme, de la conception à la mise à l'essai. En fait, les entreprises devraient instaurer une philosophie qui englobe la protection de la vie privée, la sécurité et l'éthique, et qui se traduit dans ses décisions. En plus d'accroître la confiance des employés dans l'entreprise, une telle pratique aiderait à atténuer les risques liés à l'utilisation des algorithmes. Le CDT a fait observer que, à l'heure actuelle, peu de formation est offerte aux personnes qui élaborent les algorithmes, quoique la situation s'améliore.

Les représentants de Facebook ont dit avoir mis en place des normes éthiques pour l'utilisation des algorithmes.

En ce qui concerne la quantité de renseignements personnels recueillis à l'ère des mégadonnées, les représentants du CDT ont souligné qu'il peut être utile dans certaines circonstances d'avoir beaucoup de données, mais que l'hypothèse selon laquelle il vaut toujours mieux avoir beaucoup de données est fausse. De plus, les représentants du CDT ont mentionné que l'exactitude des données recueillies et utilisées, ainsi que les taux d'erreur et les mesures de redressement à l'intention des particuliers sont des questions importantes dont il faut tenir compte. Quoi qu'il en soit, M. Beales a maintenu que, dans le contexte des mégadonnées, mieux vaut avoir des données en quantité, parce que cela permet de confirmer des renseignements. Il a ajouté que la question des erreurs se pose aussi lorsque les décisions sont d'origine humaine. M. Beales a fait valoir que les algorithmes doivent être envisagés du point de vue des coûts et des conséquences.

Les représentants du CDT ont insisté sur le fait que les renseignements traités par un algorithme, et l'algorithme lui-même, doivent être exacts et fiables, en utilisant

l'exemple suivant : si un algorithme est efficace à 99 % pour détecter les terroristes, cela implique que, vu le taux d'erreur de 1 %, des millions d'Américains seraient identifiés comme terroristes. M. Beales a indiqué que, si l'algorithme se trompe quelques fois, mais qu'il permet toujours d'identifier les terroristes, il pourrait être utile de l'employer pourvu que les personnes identifiées à tort n'en subissent pas trop d'inconvénients.

GLOSSAIRE

CJUE. Cour de justice de l'Union européenne

Code type. *Code type sur la protection des renseignements personnels* élaboré par le Conseil canadien des normes, qui est reproduit à l'annexe 1 de la *Loi sur la protection des renseignements personnels et les documents électroniques* et aux principes duquel les organisations ont l'obligation de se conformer

CPVP. Commissariat à la protection de la vie privée du Canada

CRTC. Conseil de la radiodiffusion et des télécommunications canadiennes

données dépersonnalisées. données agrégées et présentées de sorte qu'il soit impossible d'identifier à qui elles appartiennent (aussi appelées données « anonymisées » ou données « désidentifiées »)

droit à l'oubli. renvoie généralement à l'une ou l'autre des deux notions suivantes :

- le « droit à l'effacement », c'est-à-dire le droit au retrait d'informations sur un site Web
- le « droit au déréférencement » (aussi appelé « droit à la désindexation » ou « droit au délistage »), c'est-à-dire le droit au retrait de la page Web contenant l'information des résultats de recherche de moteurs de recherche comme Google

LCAP. *Loi canadienne anti-pourriel*

LPRP. *Loi sur la protection des renseignements personnels*, qui s'applique au secteur public

LPRPDE. *Loi sur la protection des renseignements personnels et les documents électroniques*, qui s'applique au secteur privé

RGPD. *Règlement général sur la protection des données* de l'Union européenne, qui entrera en vigueur en mai 2018

transparence algorithmique. le fait pour les utilisateurs de disposer d'une information complète sur le fonctionnement des programmes d'intelligence artificielle reliés aux sites Web qu'ils consultent, sur les données qu'ils collectent et la manière dont elles sont utilisées

UE. Union européenne

ANNEXE A
LISTE DES TÉMOINS

Organismes et individus	Date	Réunion
À titre personnel	2017/02/14	46
Robert Gary Dickson, consultant, ancien commissaire à l'information et à la protection de la vie privée de Saskatchewan		
Éloïse Gratton, associée et cochef national, Groupe de pratique Respect de la vie privée et protection des renseignements personnels, Borden Ladner Gervais		
Dentons Canada		
Chantal Bernier, avocate-conseil, Groupe mondial de la vie privée et cybersécurité		
Centre pour la défense de l'intérêt public		
Alysia Lau, conseillère juridique		
John Lawford, directeur exécutif et avocat général		
À titre personnel	2017/02/16	47
Valerie Steeves, professeur titulaire, Département de criminologie, Université d'Ottawa		
BC Freedom of Information and Privacy Association		
Vincent Gogolek, directeur général		
Commissariat à la protection de la vie privée du Canada		
Brent Homan, directeur général, enquête de la loi sur la protection des renseignements personnels et les documents		
Patricia Kosseim, avocate générale principale et directrice générale, Direction des services juridiques, des politiques, de la recherche et de l'analyse des technologies		
Daniel Therrien, commissaire à la protection de la vie privée du Canada		
Commission d'accès à l'information du Québec	2017/02/21	48
Cynthia Chassigneux, juge administrative, Surveillance		

Organismes et individus	Date	Réunion
Bureau du Commissaire à l'information et à la protection de la vie privée de la Colombie-Britannique Drew McArthur, commissaire par intérim Michael McEvoy, commissaire adjoint	2017/02/21	48
Office of the Information and Privacy Commissioner of Alberta Sharon Ashmore, avocate générale Jill Clayton, commissaire Kim Kreutzer Work, directrice, Gestion du savoir		
À titre personnel Florian Martin-Bariteau, professeur adjoint, section de common law, Faculté de droit, et directeur, Centre de recherche en droit, technologie et société, Université d'Ottawa Teresa Scassa, professeure titulaire, Chaire de recherche du Canada en droit d'information, Université d'Ottawa	2017/02/23	49
Centre for Law and Democracy Michael Karanicolas, conseiller juridique principal		
À titre personnel Colin J. Bennett, professeur de science politique, University of Victoria David Fraser, associé, McInnes Cooper Michael Geist, titulaire de la chaire de recherche du Canada en droit d'internet et du commerce électronique, Faculté de droit, Université d'Ottawa	2017/03/21	52
Association des libertés civiles de la Colombie-Britannique Micheal Vonn, directrice de la politique		
À titre personnel Jennifer Stoddart	2017/03/23	53
Association du Barreau canadien Suzanne Morin, vice-présidente, Section nationale du droit de la vie privée et de l'accès à l'information		

Organismes et individus	Date	Réunion
Clinique d'intérêt public et de politique d'Internet du Canada	2017/03/23	53
Tamir Israel, avocat-conseil à l'interne		
À titre personnel	2017/04/04	54
Vincent Gautrais, professeur titulaire, directeur du centre de recherche en droit public, Faculté de droit, Université de Montréal		
Ian Kerr, professeur et titulaire de la Chaire de recherche du Canada en éthique, droit et technologie, Université d'Ottawa		
Robert G. Parker, expert-conseil, Risk Masters International Inc.		
David Young, directeur, David Young Law		
À titre personnel	2017/04/06	55
Paige Backman, associée, Aird and Berlis LLP		
Alex Cameron, associé et président, Protection de l'information et de la vie privée, Fasken Martineau DuMoulin LLP		
Molly Reynolds, associée principale, Torys LLP		
Conseil de la radiodiffusion et des télécommunications canadiennes	2017/05/09	59
Steven Harroun, chef de l'application de la Conformité et enquêtes		
Daniel Roussy, avocat général et sous-directeur exécutif		
Bureau de la concurrence		
Morgan Currie, sous-commissaire déléguée, Direction des pratiques commerciales trompeuses		
Josephine Palumbo, sous-commissaire, Direction des pratiques commerciales trompeuses		
Ministère de l'Industrie		
Krista Campbell, directrice générale, Direction générale des politiques numérique, secteur du Spectre, Technologie de l'information et télécommunication		
Steve Joanisse, conseiller juridique, Services juridiques d'Innovation, Sciences et Développement économique Canada		

Organismes et individus	Date	Réunion
Ministère de l'Industrie Charles Taillefer, directeur, Direction générale des politiques numérique, secteur du Spectre, Technologie de l'information et télécommunication	2017/05/09	59
Association des banquiers canadiens Charles Docherty, conseiller juridique principal Linda Routledge, directrice, Consommation	2017/05/11	60
Association canadienne du marketing David Elder, conseiller juridique spécial, Protection des renseignements personnels numériques Wally Hill, vice-président, Affaires gouvernementales et des consommateurs		
Association canadienne des télécommunications sans fil Robert W.J. Ghiz, président et chef de direction		
Chambre de commerce du Canada Scott Smith, directeur, Propriété intellectuelle et politique d'innovation	2017/05/16	61
Conseil des consommateurs du Canada Dennis Hogarth, vice-président		
Association canadienne de la technologie de l'information André Leduc, vice-président, Relations gouvernementales et politiques Robert Watson, président et directeur général		
Association canadienne des compagnies d'assurances de personnes Anny Duval, conseillère juridique Frank Zinatelli, vice-président et avocat général	2017/05/30	62
Bureau d'assurance du Canada Randy Bundus, vice-président principal, conseiller juridique en chef Steven Lingard, directeur et chef de la protection des renseignements personnels, Services juridiques		

Organismes et individus	Date	Réunion
Bureau de la publicité interactive du Canada Sonia Carreno, présidente Adam Kardash, partenaire, vie privée et gestion de données Osler, Hoskin et Harcourt S.E.N.R.L., s.r.l.	2017/05/30	62
Association canadienne des archivistes Greg Kozak, représentant, Comité d'éthique	2017/06/01	63
Association des bibliothèques de recherche du Canada Donna Bourne-Tyson, présidente Susan Haigh, directrice générale		
Google Canada Colin McKay, chef, politiques publiques et relations gouvernementales		
Conseil canadien du commerce de détail Jason McLinton, vice-président, Division alimentation et affaires règlementaires		
Contrôleur européen de la protection des données Giovanni Buttarelli, contrôleur	2017/06/13	64
À titre personnel Jane Bailey, professeure, Faculté de droit, Université d'Ottawa	2017/09/25	68
Repaires jeunesse du Canada Owen Charters, président-directeur général Rachel Gouin, directrice, Recherche et politiques publiques		
Association nationale de destruction de l'information - Canada Kristjan Backman, président		
Commissariat à la protection de la vie privée du Canada Vance Lockton, analyste stratégique des politiques et recherche Regan Morris, conseiller juridique Daniel Therrien, commissaire à la protection de la vie privée du Canada	2018/02/01	88

ANNEXE B
LISTE DES MÉMOIRES

Organismes et individus

Backman, Paige

Baer, Aaron

Martin-Bariteau, Florian

Young, David

Association canadienne des archivistes

Association canadienne du marketing

Association des bibliothèques de recherche du Canada

Association du Barreau canadien

Association nationale de destruction de l'information - Canada

Centre pour la défense de l'intérêt public

Commissariat à la protection de la vie privée du Canada

Option consommateurs

Repaires jeunesse du Canada

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 n^{os} 46, 47, 48, 49, 52, 53, 54, 55, 59, 60, 61, 62, 63, 64, 68, 70, 79, 87, 88, 90 et 91) est déposé.

Respectueusement soumis,

Le président,
Bob Zimmer