



CHAMBRE DES COMMUNES
HOUSE OF COMMONS
CANADA

DÉMOCRATIE MENACÉE : RISQUES ET SOLUTIONS À L'ÈRE DE LA DÉSINFORMATION ET DU MONOPOLE DES DONNÉES

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

Bob Zimmer, président

**DÉCEMBRE 2018
42^e LÉGISLATURE, 1^{re} SESSION**

Publié en conformité de l'autorité du Président de la Chambre des communes

PERMISSION DU PRÉSIDENT

Les délibérations de la Chambre des communes et de ses comités sont mises à la disposition du public pour mieux le renseigner. La Chambre conserve néanmoins son privilège parlementaire de contrôler la publication et la diffusion des délibérations et elle possède tous les droits d'auteur sur celles-ci.

Il est permis de reproduire les délibérations de la Chambre et de ses comités, en tout ou en partie, sur n'importe quel support, pourvu que la reproduction soit exacte et qu'elle ne soit pas présentée comme version officielle. Il n'est toutefois pas permis de reproduire, de distribuer ou d'utiliser les délibérations à des fins commerciales visant la réalisation d'un profit financier. Toute reproduction ou utilisation non permise ou non formellement autorisée peut être considérée comme une violation du droit d'auteur aux termes de la *Loi sur le droit d'auteur*. Une autorisation formelle peut être obtenue sur présentation d'une demande écrite au Bureau du Président de la Chambre.

La reproduction conforme à la présente permission ne constitue pas une publication sous l'autorité de la Chambre. Le privilège absolu qui s'applique aux délibérations de la Chambre ne s'étend pas aux reproductions permises. Lorsqu'une reproduction comprend des mémoires présentés à un comité de la Chambre, il peut être nécessaire d'obtenir de leurs auteurs l'autorisation de les reproduire, conformément à la *Loi sur le droit d'auteur*.

La présente permission ne porte pas atteinte aux privilèges, pouvoirs, immunités et droits de la Chambre et de ses comités. Il est entendu que cette permission ne touche pas l'interdiction de contester ou de mettre en cause les délibérations de la Chambre devant les tribunaux ou autrement. La Chambre conserve le droit et le privilège de déclarer l'utilisateur coupable d'outrage au Parlement lorsque la reproduction ou l'utilisation n'est pas conforme à la présente permission.

Aussi disponible sur le site Web de la Chambre des communes à l'adresse suivante : www.noscommunes.ca

DÉMOCRATIE MENACÉE : RISQUES ET SOLUTIONS À L'ÈRE DE LA DÉSINFORMATION ET DU MONOPOLE DES DONNÉES

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

**Le président
Bob Zimmer**

DÉCEMBRE 2018

42^e LÉGISLATURE, 1^{re} 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.

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

PRÉSIDENT

Bob Zimmer

VICE-PRÉSIDENTS

Charlie Angus

Nathaniel Erskine-Smith

MEMBRES

Frank Baylis

Mona Fortier

Jacques Gourde

L'hon. Peter Kent

Joyce Murray (secrétaire parlementaire – membre sans droit de vote)

Michel Picard

Raj Saini

Anita Vandenbeld

AUTRES DÉPUTÉS QUI ONT PARTICIPÉ

Ziad Aboultaif

L'hon. Maxime Bernier

Alexandre Boulerice

Hon. Tony Clement

Don Davies

Kerry Diotte

Andy Fillmore

Greg Fergus

Iqra Khalid

Bernadette Jordan (secrétaire parlementaire – membre sans droit de vote)

Michael Levitt

Wayne Long
Alistair MacGregor
Kelly McCauley
Irene Mathysen
Brian Masse
Eva Nassif
Jean-Claude Poissant
Don Rusnak
Francis Scarpaleggia
Terry Sheehan
Marwan Tabbara
Dave Van Kesteren
Mark Warawa

GREFFIER DU COMITÉ

Michael MacPherson

BIBLIOTHÈQUE DU PARLEMENT

Service d'information et de recherche parlementaires

Alexandra Savoie, analyste

Maxime-Olivier Thibodeau, analyste

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

DIX-SEPTIÈME RAPPORT

Conformément au mandat que lui confère l'article 108(2) du Règlement, le Comité a étudié l'atteinte à la sécurité des renseignements personnels associée à Cambridge Analytica et Facebook et a convenu de faire rapport de ce qui suit :

PRÉAMBULE

À la fin du mois de mars 2018, 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 entrepris une étude sur l'atteinte à la protection des renseignements personnels impliquant Cambridge Analytica et Facebook. Le scandale a rapidement mis en lumière des questions beaucoup plus vastes concernant l'autoréglementation des monopoles de plateforme, l'utilisation de ces plateformes à des fins de collecte de données et leur rôle dans la diffusion de la désinformation et de la mésinformation dans le monde.

En juin 2018, le Comité a publié un rapport provisoire dans lequel il faisait part de ses préoccupations quant à la vulnérabilité du processus démocratique et électoral canadien à l'acquisition et à la manipulation inappropriées de données personnelles. Il a formulé huit recommandations préliminaires concernant les pouvoirs du commissaire à la protection de la vie privée du Canada, l'application de la législation sur la protection de la vie privée aux activités politiques, les exigences relatives à la transparence dans les publicités politiques, la souveraineté en matière de données et la nécessité de mieux harmoniser la législation fédérale sur la protection des renseignements personnels avec le *Règlement général sur la protection des données* de l'Union européenne (RGPD).

Le Comité a poursuivi son étude cet automne. Il a reçu des témoignages sur divers sujets, notamment les problèmes structurels inhérents aux plateformes de médias sociaux, l'interaction entre le droit de la protection de la vie privée et le droit de la concurrence dans le contexte des monopoles des données, de la cybersécurité et de la culture numérique.

Après avoir reçu d'autres témoignages, le Comité demeure d'avis que le gouvernement du Canada doit agir de toute urgence pour mieux protéger la vie privée des Canadiens. À cette fin, en plus des recommandations préliminaires présentées en juin 2018, le Comité est d'avis que le gouvernement du Canada devrait :

- soumettre les partis politiques et les tierces parties politiques à la *Loi sur la protection des renseignements personnels et les documents électroniques* (LPRPDE);
- fournir des ressources supplémentaires au Commissariat à la protection de la vie privée du Canada afin d'assurer l'exercice efficace de ses pouvoirs additionnels;

- s’assurer qu’aucun financement étranger n’a d’impact sur les élections au Canada;
- assurer la transparence dans les publicités politiques en ligne;
- imposer certaines obligations aux plateformes de médias sociaux concernant l’étiquetage du contenu produit de façon algorithmique, l’étiquetage de la publicité payante en ligne, la suppression des comptes non authentiques et frauduleux et la suppression des contenus manifestement illégaux tels que le discours haineux;
- confier à un organisme de réglementation existant ou nouveau le mandat de vérifier de façon proactive les algorithmes;
- inclure les principes de transférabilité et d’interopérabilité des données dans la LPRPDE;
- étudier les préjudices économiques potentiels causés par les monopoles de données et déterminer si la *Loi sur la concurrence* devrait être modernisée;
- étudier comment les cybermenaces affectent les institutions démocratiques et le système électoral;
- mener des recherches sur les impacts de la désinformation et de la mésinformation en ligne ainsi que sur les impacts cognitifs des produits numériques qui créent une dépendance des utilisateurs; et
- investir dans les initiatives de littératie numérique.

Comme il l’a indiqué dans son rapport préliminaire, le Comité espère que ses travaux contribueront à trouver une solution durable à un problème mondial.

TABLE DES MATIÈRES

| | |
|---|-----|
| PRÉAMBULE | vii |
| LISTE DES RECOMMANDATIONS..... | 1 |
| INTRODUCTION | 7 |
| CHAPITRE 1 : UNE ÉTUDE INATTENDUE..... | 9 |
| CHAPITRE 2 : AGGREGATE IQ | 11 |
| Nouveau témoignage de Zackary Massingham..... | 11 |
| Enquêtes menées par des organismes de surveillance et de contrôle | 12 |
| Enquête de la commission électorale du Royaume-Uni | 12 |
| Enquête du commissariat à l'information du Royaume-Uni | 13 |
| Enquêtes du commissariat à la protection de la vie privée du Canada et du commissariat à l'information et à la protection de la vie privée de la Colombie-Britannique | 18 |
| Conclusion concernant Aggregate IQ..... | 19 |
| CHAPITRE 3 : PROTECTION DES RENSEIGNEMENTS PERSONNELS ET PARTIS POLITIQUES..... | 21 |
| Application des lois relatives à la protection des renseignements personnels aux partis politiques | 21 |
| Point de vue des universitaires..... | 21 |
| Point de vue des partis politiques..... | 23 |
| Point de vue du directeur général des élections | 25 |
| Point de vue du commissaire à la protection de la vie privée..... | 25 |
| Utilisation de fonds étrangers dans les élections canadiennes | 29 |
| CHAPITRE 4 : RÉGLEMENTATION DES PLATEFORMES DE MÉDIAS SOCIAUX À L'ÈRE DE LA DÉSINFORMATION ET DE LA MÉSINFORMATION..... | 33 |
| Contrer la propagation de désinformation et de mésinformation en ligne..... | 33 |

| | |
|---|----|
| Transformation de l'écosystème d'information | 33 |
| Problèmes structurels des plateformes de médias sociaux..... | 35 |
| Insuffisance de l'autoréglementation | 38 |
| Risques liés à la réglementation | 40 |
| Solutions réglementaires potentielles..... | 42 |
| Transparence en matière de publicité en ligne | 42 |
| Transparence des algorithmes et responsabilité à l'égard du contenu | 44 |
| Modération du contenu..... | 47 |
| Contrôle et consentement de l'utilisateur | 48 |
| CHAPITRE 5 : UN RÉGULATEUR INDÉPENDANT? | 49 |
| Les plateformes de médias sociaux comme diffuseurs..... | 49 |
| Normes concernant la modération du contenu en ligne..... | 51 |
| CHAPITRE 6 : RÉGLEMENTATION DU POUVOIR MONOPOLISTIQUE DES GÉANTS DE LA TECHNOLOGIE ET DU MONOPOLE DES DONNÉES | 53 |
| Témoignages pertinents | 53 |
| Maurice Stucke | 53 |
| Bureau de la concurrence | 57 |
| Banque du Canada..... | 60 |
| Ben Scott, Tristan Harris et Colin McKay | 62 |
| Conclusions et recommandations | 63 |
| CHAPITRE 7: CYBERSÉCURITÉ | 65 |
| Témoignages pertinents | 65 |
| Centre de la sécurité des télécommunications | 65 |
| Témoignage de Ben Scott | 67 |
| Témoignage de Maurice Stucke | 68 |
| Témoignages de Michael Pal et du directeur général des élections | 68 |
| Conclusions et recommandations | 69 |

| | |
|---|----|
| CHAPITRE 8 : RECHERCHE, LITTÉRATIE NUMÉRIQUE ET SENSIBILISATION DU PUBLIC | 71 |
| Absence de recherche | 71 |
| Littératie numérique | 73 |
| Sensibilisation du public..... | 74 |
| CONCLUSION | 79 |

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.

Recommandation 1

Que le gouvernement du Canada modifie la *Loi sur la protection des renseignements personnels et les documents électroniques* pour y assujettir les partis politiques tout en tenant compte de leurs obligations de mener des activités d'information et de sensibilisation démocratique. 28

Recommandation 2

Que le gouvernement du Canada modifie la *Loi sur la protection des renseignements personnels et les documents électroniques* pour y assujettir les tierces parties politiques. 28

Recommandation 3

Que le gouvernement du Canada octroie le mandat et l'autorité au commissaire à la protection de la vie privée ou à Élections Canada de mener des audits proactifs des partis politiques et des tierces parties politiques à l'égard de leurs pratiques relatives à la protection des renseignements personnels et d'émettre des ordonnances et des sanctions monétaires. 28

Recommandation 4

Que le gouvernement du Canada fournisse les ressources additionnelles nécessaires au Commissariat à la protection de la vie privée afin qu'il puisse faire face aux problèmes modernes liés à la protection de la vie privée et exercer de façon efficace les pouvoirs additionnels octroyés au commissaire..... 29

Recommandation 5

Que le gouvernement du Canada prenne toutes les mesures nécessaires afin de prévenir le financement étranger et l'influence étrangère dans les élections au Canada, y compris le financement étranger provenant d'organismes de bienfaisance enregistrés. 31

Recommandation 6

Que le gouvernement du Canada modifie la *Loi électorale du Canada* pour obliger un mandataire à soumettre une pièce d'identité et une preuve d'adresse lors de la mise en ligne de publicités politiques. 44

Recommandation 7

Que le gouvernement du Canada modifie la *Loi électorale du Canada* pour obliger les plateformes de médias sociaux à s'assurer que les bases de données consultables et lisibles par machine de publicités politiques en ligne qu'elles créent soient faciles à naviguer et permettent à quiconque de trouver des publicités à l'aide de filtres tels que : la personne qui a financé l'annonce, la question politique couverte, la période pendant laquelle l'annonce était en ligne, et la démographie du public cible. 44

Recommandation 8

Que le gouvernement du Canada adopte une loi visant à réglementer les plateformes de médias sociaux en utilisant comme modèle les seuils de portée au Canada décrits au paragraphe 325.1(1) du projet de loi C-76, Loi modifiant la Loi électorale du Canada et d'autres lois et apportant des modifications corrélatives à d'autres textes législatifs. Parmi ces responsabilités, devrait être inclus un devoir :

- d'étiqueter clairement le contenu produit automatiquement ou algorithmiquement (p.ex. par des « robots ») ;
- de détecter et supprimer les comptes non authentiques et frauduleux qui se font passer pour d'autres pour des raisons malveillantes ;
- de respecter un code de pratique qui interdirait les pratiques trompeuses ou injustes et qui exigerait une réponse rapide aux signalements de harcèlement, de menaces et de discours haineux, et l'obligation de retirer le contenu diffamatoire, frauduleux et manipulé à des fins malveillantes (p. ex. les vidéos contrefait appelés « deep fake ») ; et
- d'étiqueter clairement la publicité politique ou autre publicité payante. 46

Recommandation 9

Que le gouvernement du Canada édicte des exigences en matière de transparence en ce qui concerne les algorithmes et fournisse à un organisme de réglementation existant ou nouveau le mandat et l'autorité de faire des vérifications d'algorithmes. 46

Recommandation 10

Que le gouvernement du Canada introduise une loi imposant une obligation aux plateformes de médias sociaux de retirer, dans un délai raisonnable, le contenu manifestement illégal qui s'y retrouve, incluant le discours incitant à la haine, le harcèlement et la désinformation, sous peine de faire face à une sanction monétaire imposée en fonction d'une échelle de responsabilité proportionnelle à la dominance et à l'importance de la plateforme sociale et qui prévoit une supervision judiciaire du retrait de contenu et un droit d'appel. 47

Recommandation 11

Que la *Loi sur la protection des renseignements personnels et les documents électroniques* soit modifiée en y ajoutant les principes relatifs à la portabilité des données et à l'interopérabilité des systèmes. 64

Recommandation 12

Que le gouvernement du Canada étudie les dommages économiques potentiellement causés par les soi-disant « monopoles de données » au Canada et qu'il détermine si la modernisation de la *Loi sur la concurrence* est requise. 64

Recommandation 13

Que la *Loi sur la protection des renseignements personnels et les documents électroniques* et la *Loi sur la concurrence* soient modifiées afin d'établir un cadre permettant au Bureau de la concurrence et au Commissariat à la protection de la vie privée de collaborer lorsqu'il est approprié de le faire. 64

Recommandation 14

Que les partis politiques suivent les recommandations du Centre de la sécurité des télécommunications qui les concernent en matière de cybersécurité électorale. 69

Recommandation 15

Que le gouvernement du Canada continue d'étudier la manière dont les cybermenaces affectent les institutions et le système électoral du Canada. 69

Recommandation 16

Que le gouvernement du Canada investisse des ressources dans la recherche sur les impacts de la désinformation et de la mésinformation en ligne..... 75

Recommandation 17

Que le gouvernement du Canada augmente ses investissements en matière d'initiatives de littératie numérique, y compris à l'égard d'initiatives visant à informer les Canadiens des risques liés à la propagation de désinformation et de mésinformation en ligne..... 75

Recommandation 18

Que le gouvernement du Canada étudie les effets cognitifs à long terme des produits numériques favorisant la dépendance qui sont offerts par les plateformes sociales, et qu'il détermine si une réponse est requise. 76

Recommandation 19

Que le gouvernement du Canada établisse des exigences sur la transparence relativement à la collecte et à l'utilisation des données que font les organisations et les acteurs politiques, particulièrement au moyen des médias sociaux et d'autres plateformes en ligne afin de cibler la publicité politique ou autre à l'aide de techniques comme le profilage psycho-graphique. Ces exigences pourraient inclure, sans s'y limiter :

- L'identification de la personne qui a payé pour la publicité, y compris la vérification de l'authenticité de la personne qui diffuse la publicité; 76**
- L'identification du public cible et la raison pour laquelle le public cible a reçu la publicité; et**
- L'enregistrement obligatoire concernant la publicité politique à l'extérieur du Canada. 77**

Recommandation 20

Que le gouvernement du Canada mette immédiatement en œuvre des mesures pour veiller à ce que des protections semblables à celles du *Règlement général sur la protection des données* soient mises en place au Canada, y compris les recommandations contenues dans le rapport sur la *Loi sur la protection des renseignements personnels et les documents électroniques* présenté en février 2018..... 77

Recommandation 21

Que le gouvernement du Canada établisse des règles et des lignes directrices sur la propriété des données et la souveraineté des données afin de mettre un terme à la collecte et à l'utilisation non autorisées des renseignements personnels des citoyens. Ces règles et lignes directrices devraient tenir compte des défis que représente l'infonuagique. 77

Recommandation 22

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. 77

Recommandation 23

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. 77

Recommandation 24

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 d'émettre des avis urgents à une organisation relativement à la production de documents pertinents dans une durée plus courte et le pouvoir de saisir des documents dans le cadre d'une enquête, sans préavis. 78

Recommandation 25

Que la *Loi sur la protection des renseignements personnels et les documents électroniques* soit modifiée afin d'autoriser le commissaire à la protection de la vie privée à partager certaines informations pertinentes dans le cadre d'enquêtes avec le Bureau de la concurrence, d'autres organismes de régulation canadiens et des organismes de régulation à l'échelle internationale, lorsque cela est approprié. 78

Recommandation 26

Que le gouvernement du Canada prenne certaines mesures afin d'assurer l'application de la législation en matière de protection de la vie privée aux activités politiques, soit par la modification des lois existantes ou par l'adoption d'une nouvelle loi. 78



INTRODUCTION

Le 17 avril 2018, 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 débuté son étude relative à l'atteinte à la sécurité des renseignements personnels impliquant Cambridge Analytica et Facebook (« l'atteinte à la sécurité »). Rapidement, le Comité a compris que cette atteinte à la sécurité ne représentait que la pointe de l'iceberg et soulevait une myriade de questions importantes.

Le 19 juin 2018, le Comité a présenté à la Chambre des communes un rapport provisoire intitulé *Aborder les vulnérabilités de la vie privée numérique et les menaces potentielles au processus électoral démocratique canadien* qui visait à dévoiler les travaux du Comité à cette date et à faire plusieurs recommandations préliminaires.

Du 25 septembre au 1^{er} novembre 2018, le Comité a poursuivi son étude dans le but d'explorer davantage certains des sujets abordés et d'étudier d'autres questions qui ont émergé de la première série de témoignages. Cette preuve additionnelle permet au Comité de présenter son rapport final.

En tout, le Comité aura consacré 18 réunions publiques à cette étude au cours de laquelle il a entendu 47 témoins, certains ayant comparu plus d'une fois. Il a également reçu 2 mémoires.

CHAPITRE 1 : UNE ÉTUDE INATTENDUE

Comme des millions de Canadiens, le Comité a été surpris par la révélation, en mars 2018, de l'atteinte à la sécurité. Même si des questions à l'égard des pratiques des plateformes de médias sociaux en matière de collecte de renseignements personnels avaient déjà été soulevées auparavant, la révélation de l'atteinte à la sécurité, qui aurait permis la collecte d'environ 87 millions de profils d'utilisateurs Facebook, a envoyé une onde de choc dans le monde. Elle a soulevé les passions de plusieurs universitaires, journalistes et citoyens, mené à des enquêtes, en plus de susciter l'engouement de comités parlementaires d'ici et d'ailleurs.

Le Comité s'est d'abord concentré sur l'atteinte à la sécurité et la possibilité que des Canadiens aient été affectés. Il a entendu les témoignages des parties intéressées, soit Facebook, Aggregate IQ (« AIQ »), Christopher Wylie et Chris Vickery, un expert en cybersécurité qui a découvert une base de données appartenant à AIQ en ligne. Le Comité a également invité certains commissaires menant une enquête à l'égard de l'atteinte à la sécurité à témoigner, soit le commissaire à la protection de la vie privée du Canada (« CPVP »), le commissaire à l'information et à la protection de la vie privée de la Colombie-Britannique et la commissaire à l'information du Royaume-Uni.

Le Comité a aussi entendu le président du Comité du numérique, de la culture, des médias et du sport du Royaume-Uni (le « Comité du Royaume-Uni »), Damian Collins, dont le comité mène une étude sur la désinformation. Le Comité du Royaume-Uni avait un intérêt particulier envers AIQ, une entreprise canadienne qui a joué un rôle dans le référendum sur le Brexit. Le Comité a cherché à éclaircir la situation relative à AIQ. Ces efforts et les conclusions du Comité à cet égard sont présentés dans le second chapitre du présent rapport.

Enfin, le Comité a aussi entendu le point de vue d'experts, d'universitaires, ainsi que de représentants d'autres plateformes et de l'industrie des technologies. Ces témoignages ont enrichi la discussion, soulevé des pistes de solution et suscité des questions additionnelles dont nous traitons dans le présent rapport. Les témoignages entendus par le Comité entre avril et juin 2018 lui ont permis de faire 8 recommandations préliminaires¹.

1 Les recommandations préliminaires sont incluses dans le présent rapport final et se retrouvent à la fin du chapitre 8 en tant que recommandations 19 à 26.



CHAMBRE DES COMMUNES
HOUSE OF COMMONS
CANADA

Bâtissant sur ses recommandations préliminaires et à la lumière des nouveaux témoignages entendus, le Comité réitère les recommandations faites en juin 2018 et en propose de nouvelles afin d'atténuer la menace qui guette la démocratie dans l'ère de la désinformation et des monopoles des données. Le Comité espère que le fruit de son travail aidera le gouvernement du Canada à mieux comprendre les enjeux auxquels le Canada fait face et l'incitera à agir.

CHAPITRE 2 : AGGREGATE IQ

NOUVEAU TÉMOIGNAGE DE ZACKARY MASSINGHAM

Le 27 septembre 2018, Zackary Massingham, qui est le directeur général d'AIQ, a comparu devant le Comité. Il avait déjà comparu le 24 avril 2018 en compagnie de Jeff Silvester, qui est le chef des opérations d'AIQ. M. Silvester a comparu à nouveau, seul, le 12 juin 2018. Lors de sa comparution du 27 septembre, M. Massingham a essentiellement fait les mêmes affirmations que M. Silvester et lui avaient faites lors de leurs comparutions précédentes.

En somme, ces affirmations sont à l'effet qu'AIQ n'est aucunement reliée à Cambridge Analytica ou SCL Group (SCL), qu'ils n'ont jamais vu de preuve d'une coordination entre les organisations Vote Leave et BeLeave dans le cadre de la campagne pour le Brexit, et qu'ils n'avaient aucune connaissance du fait que les renseignements personnels fournis par SCL avaient été obtenus de Facebook illégalement.

Le Comité estime que les représentants d'AIQ, autant individuellement qu'ensemble, n'ont pas fourni de réponses satisfaisantes à ses questions. Il est d'avis que la preuve reçue demeure problématique à plusieurs égards.

Dans son rapport provisoire présenté en juin 2018, le Comité avait noté qu'il n'adhérait pas à la version des faits présentée par les représentants d'AIQ à ce stade parce que leur témoignage était inconstant et parsemé de contradictions et qu'il allait à l'encontre du témoignage de plusieurs témoins crédibles². Le Comité avait également noté un manque de coopération de la part des représentants d'AIQ à une période de l'enquête de la commissaire à l'information du Royaume-Uni, Elizabeth Denham³.

2 Comité permanent de l'accès à l'information, de la protection des renseignements personnels et de l'éthique (ETHI), *Aborder les vulnérabilités de la vie privée numérique et les menaces potentielles au processus électoral démocratique canadien*, p. 20.

3 *Ibid.*, p. 21.



ENQUÊTES MENÉES PAR DES ORGANISMES DE SURVEILLANCE ET DE CONTRÔLE

Enquête de la commission électorale du Royaume-Uni

Le 17 juillet 2018, la commission électorale du Royaume-Uni, un organisme indépendant qui supervise les élections et les référendums et contrôle le financement politique, a publié un rapport d'enquête sur les dépenses et le financement relatifs à la campagne du référendum sur le Brexit en 2016⁴. Bien que l'enquête de la commission électorale n'ait pas porté directement sur AIQ ou sur ses représentants, l'entreprise se retrouve au cœur de cette enquête qui portait principalement sur cinq paiements faits à AIQ en juin 2016⁵.

En ce qui concerne le lien entre les dépenses de Darren Grimes, de BeLeave et de Vote Leave, sur qui portait directement l'enquête, la commission électorale est parvenue à la conclusion suivante :

La Commission est convaincue, hors de tout doute raisonnable, que la totalité des dépenses faites par M. Grimes et BeLeave lors de la campagne référendaire ont été enregistrées dans le cadre d'un plan commun avec Vote Leave. Ces dépenses, y compris la somme de 675 315,18 livres sterling consacrée à des services d'Aggregate IQ et déclarée par M. Grimes, auraient dû être considérées comme des dépenses de Vote Leave⁶.

Le fait d'associer ainsi les dépenses de M. Grimes et de BeLeave à celles de Vote Leave a mené la commission électorale à constater que Vote Leave avait dépassé la limite de dépenses électorales permise par la loi applicable⁷.

Le rapport de la commission électorale conclut également que Veterans for Britain a déclaré de manière inexacte et illégale avoir reçu et accepté un don de 100 000£ en argent comptant le 20 mai 2016, alors qu'il s'agissait en réalité d'un virement fait par Vote Leave directement à AIQ le 29 juin 2016 pour des services fournis à Veterans for Britain lors des derniers jours de la campagne du référendum sur le Brexit⁸.

4 Royaume-Uni, The Electoral Commission, [*Report of an investigation in respect of - Vote Leave Limited - Mr Darren Grimes - BeLeave - Veterans for Britain Concerning campaign funding and spending for the 2016 referendum on the UK's membership of the EU*](#), 17 juillet 2018 [DISPONIBLE EN ANGLAIS SEULEMENT].

5 *Ibid.*, para. 1.12, p. 5.

6 *Ibid.*, para. 1.14 et para. 4.1, p. 16. [TRADUCTION]

7 *Ibid.*, para. 1.16, p. 6 et para. 4.25, p. 21.

8 *Ibid.*, para. 1.23, p. 7 et para. 4.63, p. 28.

À cet égard, la commission estime que, bien que les représentants de Vote Leave et de Veterans for Britain se connaissaient et collaboraient et que Vote Leave avait recommandé les services d'AIQ à Veterans for Britain, « les preuves que nous avons obtenues ne soutiennent pas l'affirmation selon laquelle les services auraient été fournis à Veterans for Britain dans le cadre d'une collaboration avec Vote Leave⁹ ».

En outre, la commission électorale tire la conclusion suivante en ce qui a trait à la coordination entre les parties impliquées et au traitement des données par AIQ :

La capacité de BeLeave d'obtenir des services d'Aggregate IQ reposait entièrement sur les mesures prises par Vote Leave pour lui verser des dons et prévoir un donateur distinct pour l'organisation. Même s'il est possible que BeLeave ait apporté sa contribution sous la forme du style ou du contenu, les services fournis par Aggregate IQ à BeLeave ont utilisé les messages de Vote Leave sur l'ordre du directeur de campagne de BeLeave. Ces services semblent aussi avoir profité des données de Vote Leave et/ou de données obtenues à partir de ressources en ligne que Vote Leave a mises sur pied et fournies à BeLeave afin de cibler et de distribuer son matériel de campagne. Ce constat s'appuie sur des preuves provenant de Facebook selon lesquelles Aggregate IQ a utilisé des listes de cibles identiques pour les publicités de Vote Leave et de BeLeave, quoique celles de BeLeave n'ont pas été diffusées¹⁰.

Enfin, la commission électorale souligne dans son rapport que la preuve ne supporte pas les affirmations de Vote Leave et de BeLeave à l'effet que les paiements faits par BeLeave à AIQ représentaient des dons et que Vote Leave n'avait eu aucune influence sur l'utilisation que BeLeave en avait faite¹¹.

Enquête du commissariat à l'information du Royaume-Uni

Le 6 novembre 2018, le commissariat à l'information du Royaume-Uni, a présenté un rapport au parlement britannique à propos de son enquête sur l'utilisation de l'analyse de données dans les campagnes politiques¹². Le même jour, la commissaire à l'information, Elizabeth Denham, comparaissait devant le Comité du Royaume-Uni pour notamment lui faire part des conclusions de son enquête¹³.

9 *Ibid.*, para. 1.24. Voir aussi *Ibid.*, para. 4.69, p. 29. [TRADUCTION]

10 *Ibid.*, para. 4.19. [TRADUCTION]

11 *Ibid.*, para. 4.20, p. 20.

12 Royaume-Uni, Information Commissioner's Office, *Investigation into the use of data analytics in political campaigns A report to Parliament*, 6 novembre 2018 [DISPONIBLE EN ANGLAIS SEULEMENT].

13 Royaume-Uni, Parlement, *Digital, Culture, Media and Sport Committee*, 6 novembre 2018 [DISPONIBLE EN ANGLAIS SEULEMENT].



Le 11 juillet 2018, le commissariat avait publié un rapport provisoire sur la progression de son enquête à la demande du Comité du Royaume-Uni¹⁴. Le même jour, le commissariat avait également publié un rapport contenant des recommandations en matière de politiques publiques qui découlent de cette enquête¹⁵.

Le 24 octobre 2018, le commissariat a imposé à Facebook une amende de 500 000£ en raison d'atteintes graves à la loi applicable en matière de protection des données¹⁶. L'imposition de cette amende découle de l'enquête du commissariat à l'information sur l'utilisation de l'analyse de données dans les campagnes politiques. M^{me} Denham a expliqué qu'elle a décidé d'imposer le montant le plus élevé disponible dans la législation en vigueur au moment des faits, en raison de la gravité des actes reprochés à Facebook, tout en soulignant que ce montant aurait été beaucoup plus élevé si le *Règlement général sur la protection des données* (RGPD) avait été en vigueur¹⁷. En effet, la *Data Protection Act 1998* qui a été appliquée pour imposer cette amende a été remplacée au Royaume-Uni en mai 2018 par la nouvelle loi intitulée *Data Protection Act 2018* et par le RGPD, qui prévoient des amendes maximales de 17 millions de livres ou 4% des revenus mondiaux de l'entreprise visée¹⁸.

Les conclusions du commissariat à l'endroit de Facebook en lien avec cette amende – et avec le sujet de la présente étude du Comité – sont sévères :

L'enquête du commissariat à l'information a révélé que, entre 2007 et 2014, Facebook a traité incorrectement les renseignements personnels de ses utilisateurs en permettant aux développeurs d'applications d'accéder à ces renseignements sans qu'un consentement suffisamment clair et éclairé soit donné, et en permettant même l'accès aux renseignements des utilisateurs qui n'avaient pas téléchargé l'application, mais qui étaient simplement « amis » d'utilisateurs qui l'avaient téléchargée.

Facebook a aussi omis de protéger les renseignements personnels en n'effectuant pas les vérifications requises des applications et des développeurs utilisant sa plateforme.

14 Royaume-Uni, Information Commissioner's Office, , *Investigation into the use of data analytics in political campaigns Investigation update*, 11 juillet 2018 [DISPONIBLE EN ANGLAIS SEULEMENT].

15 Royaume-Uni, Information Commissioner's Office, *Democracy disrupted? Personal information and political influence*, 11 juillet 2018 [DISPONIBLE EN ANGLAIS SEULEMENT].

16 Royaume-Uni, Information Commissioner's Office, *ICO issues maximum £500,000 fine to Facebook for failing to protect users' personal information*, 25 octobre 2018 [DISPONIBLE EN ANGLAIS SEULEMENT]. Voir aussi l'avis d'imposition d'une amende : Royaume-Uni, Information Commissioner's Office, *Data Protection Act 1998 Supervisory Powers of the Information Commissioner Monetary Penalty Notice*, 24 octobre 2018 [DISPONIBLE EN ANGLAIS SEULEMENT].

17 Royaume-Uni, Information Commissioner's Office, *ICO issues maximum £500,000 fine to Facebook for failing to protect users' personal information*, 25 octobre 2018 [DISPONIBLE EN ANGLAIS SEULEMENT].

18 *Ibid.*

En raison de ce manquement à la sécurité, Aleksandr Kogan et son entreprise GSR ont recueilli les données Facebook de jusqu'à 87 millions de personnes dans le monde, à leur insu. Une certaine partie de ces données a ensuite été transmise à d'autres organisations, dont le SCL Group – la société-mère de Cambridge Analytica – qui ont contribué à des campagnes électorales aux États-Unis.

Même après que l'utilisation abusive des données a été mise au jour en décembre 2015, Facebook n'a pas fait tout le nécessaire pour s'assurer que les organisations qui détenaient toujours ces données avaient pris des mesures correctives adéquates en temps opportun, y compris la suppression des données. Dans le cas du SCL Group, ce n'est qu'en 2018 que Facebook a suspendu l'entreprise de sa plateforme¹⁹.

Le rapport du 6 novembre présente notamment les résultats de l'enquête du commissariat à l'information sur les liens entre AIQ, SCL Elections (SCLE) et Cambridge Analytica (CA). Le rapport note qu'AIQ a expliqué au commissariat que l'entièreté de son travail avait été accompli en traitant avec SCLE et non avec CA. Le rapport note également que l'examen par le commissariat des données récupérées à ce stade n'avait révélé aucune preuve que des renseignements personnels, y compris ceux de citoyens du Royaume-Uni, avaient été partagés par CA avec AIQ²⁰. Le rapport tire la conclusion suivante quant à la personnalité juridique d'AIQ :

Même si les organisations entretenaient clairement une relation de travail étroite et que plusieurs de leurs employés étaient connus de l'une comme de l'autre, nous ne disposons d'aucune preuve indiquant qu'AIQ était autre chose qu'une entité juridique distincte.

Nous pouvons cependant comprendre les préoccupations plus générales exprimées relativement à la collaboration étroite entre les entreprises, qui découlent des renseignements communs sur les coordonnées indiquées dans les sites Web des entreprises et sur les modalités de paiement²¹.

Le rapport conclut que la relation entre AIQ et SCLE était une relation contractuelle et indique qu'aucune preuve d'activité illégale en lien avec les renseignements personnels de citoyens du Royaume-Uni et le travail d'AIQ auprès de SCLE n'a été trouvée et qu'à ce jour il n'y a aucune preuve que ces entités ont été impliquées dans l'analyse de données dans le cadre de campagnes liées au référendum sur le Brexit²².

19 *Ibid.* [TRADUCTION]

20 Royaume-Uni, Information Commissioner's Office, *Investigation into the use of data analytics in political campaigns A report to Parliament*, 6 novembre 2018, p. 41 [DISPONIBLE EN ANGLAIS SEULEMENT].

21 *Ibid.* [TRADUCTION]

22 *Ibid.*, p. 42.



Selon la première version du rapport, ces conclusions ont été confirmées par le commissariat à la protection de la vie privée du Canada (CPVP). En ce qui concerne les enquêtes menées conjointement par le CPVP et le commissariat à l'information et à la protection de la vie privée de la Colombie-Britannique (CIPVP) sur Facebook et AIQ, dont il est plus amplement question plus loin dans ce chapitre, le rapport mentionne que les commissariats canadiens ont avisé le commissariat britannique qu'ils n'ont pas trouvé de renseignements personnels de citoyens du Royaume-Uni, autre que ceux identifiés dans l'avis d'application de la loi²³. Le commissariat a apporté des corrections à son rapport et a publié la déclaration suivante sur son site Web : « le rapport reconnaît maintenant la contribution du commissariat à la protection de la vie privée du Canada et celle du commissariat à l'information et à la protection de la vie privée de la Colombie-Britannique à l'égard de la conclusion concernant les citoyens du R.-U. Leurs enquêtes sont toujours en cours et ils ne sont pas encore parvenus à leurs conclusions²⁴ ».

Le rapport mentionne qu'en réponse à une demande d'information du commissariat, Facebook a confirmé qu'AIQ avait créé et placé de la publicité pour le compte de la campagne « Vote to Leave » du Democratic Unionist Party (DUP), de Vote Leave, de BeLeave et de Veterans for Britain²⁵. Le rapport mentionne également que :

En réponse à notre demande d'information, Facebook a fait savoir que les adresses de courriel ne provenaient pas des données recueillies à l'aide de l'application d'Aleksandr Kogan, mais d'une autre source...

Facebook a confirmé que Vote Leave et BeLeave utilisaient le même ensemble de données afin de déterminer les publics cibles et de sélectionner les critères de production des publicités. BeLeave n'a toutefois pas diffusé de publicité en se servant de cet ensemble de données. Le rapport du 17 juillet 2018 de la commission électorale confirme que BeLeave n'a pas présenté de rapport de campagne²⁶.

La commissaire Denham explique qu'elle s'est penchée sur la question de savoir dans quelle mesure – et sur quelle base – AIQ et SCLE avaient échangé les renseignements personnels d'électeurs britanniques entre elles et avec d'autres dans le but de cibler les publicités en question. La commissaire explique également avoir partagé de la preuve pertinente et appropriée avec la commission électorale, qui s'est penchée sur les

23 *Ibid.*, p.49.

24 Royaume-Uni, Information Commissioner's Office, Investigation into data analytics for political purposes. [TRADUCTION]

25 *Ibid.*, p. 48.

26 *Ibid.*, p. 50. [TRADUCTION]

allégations de coordination entre Vote Leave et BeLeave et sur la question de la violation des règles électorales, comme l'explique la première partie de ce chapitre²⁷.

En ce qui concerne les enquêtes de police en cours qui sont reliées à cette affaire, le rapport affirme que :

La commission électorale a demandé à la police de faire enquête sur certaines personnes; pour cette raison, celles-ci refusent pour le moment de contribuer à notre enquête. Lorsque les enquêtes policières seront terminées, nous reprendrons ce volet de notre enquête afin d'éclaircir toute question relative à la protection des données²⁸.

Le rapport explique qu'à la suite de l'avis d'application de la loi révisé qu'a émis le commissariat le 24 octobre 2018, qui contenait des instructions précises à l'endroit d'AIQ et qui a permis d'étendre l'enquête du commissariat, ce dernier n'a trouvé aucune preuve que des renseignements personnels de citoyens britanniques avaient été traités illégalement²⁹.

Le rapport rappelle toutefois le manque de coopération d'AIQ dans le passé, que la lettre d'AIQ au commissariat du 5 mars 2018 avait rendu évident en affirmant qu'AIQ n'était pas assujettie à l'autorité du commissariat à l'information du Royaume-Uni et qu'elle considérait son implication dans l'enquête comme étant terminée. Cette situation avait d'ailleurs été dénoncée au Comité par la commissaire Denham lors de la première comparution d'AIQ devant le Comité³⁰. Le rapport note que la situation s'est améliorée par la suite, AIQ acceptant de coopérer entièrement par rapport à l'enquête depuis le mois d'avril 2018³¹.

En ce qui concerne le travail fait par AIQ pour le compte de BeLeave, Veterans for Britain et Vote Leave, le rapport conclut qu'aucune preuve n'a été trouvée à l'effet que des renseignements personnels aient été traités illégalement, transférés à l'extérieur du Royaume-Uni ou encore traités sans le consentement des personnes concernées³².

Cependant, le rapport fait la mise en garde suivante à propos des actions de Vote Leave :

27 Ibid.

28 Ibid. [TRADUCTION]

29 Ibid., p. 51-52.

30 Ibid., p.52. Voir : ETHI, *Aborder les vulnérabilités de la vie privée numérique et les menaces potentielles au processus électoral démocratique canadien*, p. 22.

31 Ibid.

32 Ibid., p. 52-53.



Nous examinons comment Vote Leave a diffusé ses communications promotionnelles électroniques et si la conduite de l'organisation a contrevenu au *Privacy and Electronic Communications Regulations* [Règlement sur la protection de la vie privée et les communications électroniques]. Nous avons des préoccupations à cet égard, et nous présenterons sous peu un rapport sur le sujet³³.

Dans l'éventualité où de nouvelles informations qui l'intéressent seraient publiées par le commissariat à l'information du Royaume-Uni, le Comité se réserve la possibilité de rouvrir la présente étude ou d'en entreprendre une autre en se fondant sur ces nouvelles informations.

Enquêtes du commissariat à la protection de la vie privée du Canada et du commissariat à l'information et à la protection de la vie privée de la Colombie-Britannique

Comme mentionné précédemment et comme l'explique le rapport provisoire du Comité de juin 2018, le CPVP et le CIPVP mènent conjointement leurs enquêtes sur Facebook et AIQ³⁴.

Le 10 mai 2018, le Comité a reçu le témoignage du commissaire à l'information et à la protection de la vie privée de la Colombie-Britannique, Michael McEvoy³⁵. Le Comité a entendu le commissaire à la protection de la vie privée du Canada, Daniel Therrien, le 17 avril et le 31 mai 2018. Il l'a entendu à nouveau le 1^{er} novembre 2018, à la toute fin de son étude.

Lors de sa comparution du 1^{er} novembre, M. Therrien a affirmé à l'égard de son enquête menée de concert avec le CIPVP que le travail avance bien, mais qu'ils n'ont pas encore tiré de conclusions. Ils continuent de recueillir et d'analyser l'information.

Notre enquête sur AggregatIQ porte sur la collecte ou l'utilisation de renseignements personnels sans consentement, ou à des fins autres que celles identifiées ou évidentes pour les personnes. Depuis ma dernière comparution, les enquêteurs du Commissariat ont formulé d'autres demandes de renseignements. Ils ont fait une visite des lieux. Ils ont mené des entrevues sous serment avec M. Massingham et M. Silvester, et ils ont examiné des centaines de dossiers internes d'AggregatIQ, entre autres ceux contenus dans ses appareils électroniques.

33 *Ibid.*, p. 53. [TRADUCTION]

34 ETHI, *Aborder les vulnérabilités de la vie privée numérique et les menaces potentielles au processus électoral démocratique canadien*, p. 28-29.

35 *Ibid.*, p. 31.

Afin de rendre nos conclusions publiques le plus tôt possible, nous prévoyons de procéder en deux phases, une à la fin de cette année civile — le mois prochain — et une deuxième phase au printemps³⁶.

CONCLUSION CONCERNANT AGGREGATE IQ

À la lumière des conclusions finales du CPVP et du CIPVP à venir dans cette affaire, le Comité jugera s'il est opportun de rouvrir la présente étude ou d'en entreprendre une autre sur de nouvelles bases.

36 ETHI, *Témoignages*, 1^{re} session, 42^e législature, 1^{er} novembre 2018 (Daniel Therrien, commissaire à la protection de la vie privée du Canada).

CHAPITRE 3 : PROTECTION DES RENSEIGNEMENTS PERSONNELS ET PARTIS POLITIQUES

APPLICATION DES LOIS RELATIVES À LA PROTECTION DES RENSEIGNEMENTS PERSONNELS AUX PARTIS POLITIQUES

Dans son rapport provisoire, le Comité a recommandé au gouvernement du Canada de prendre des mesures afin d'assurer l'application de la législation en matière de protection de la vie privée aux activités politiques. Il a entendu des témoignages additionnels à ce sujet à l'automne.

Point de vue des universitaires

Fenwick McKelvey, professeur agrégé en communications à l'Université Concordia, appuie la recommandation du Comité voulant que les lois en matière de protection des renseignements personnels s'appliquent à tous les partis politiques. Il recommande l'adoption d'un code de déontologie afin d'améliorer la politique canadienne³⁷. À son avis, ne pas soumettre les partis politiques à la *Loi sur la protection des renseignements personnels et les documents électroniques* (LPRDPE) est une erreur puisqu'il s'agirait d'une « solution très facile, et nous voyons que c'est efficace en Colombie-Britannique »³⁸.

Elizabeth Dubois, professeure adjointe du Département de communication de l'Université d'Ottawa, a noté que les entités politiques recueillent des données continuellement et non pas uniquement dans le cadre de campagnes électorales. Elle concède que l'utilisation de données par les entités politiques n'est pas toujours néfaste, mais suggère que « pour équilibrer le pour et le contre » d'une telle utilisation « il sera crucial de viser aussi les partis politiques dans les lois sur l'utilisation des données personnelles en vigueur, surtout dans la *Loi sur la protection des renseignements personnels et les documents électroniques* »³⁹. Elle ajoute qu'il faudra également ajouter

37 ETHI, *Témoignages*, 1^{re} session, 42^e législature, 25 septembre 2018, 1115 (Fenwick McKelvey, professeur agrégé, Études en communications, Université Concordia).

38 *Ibid.*, 1140.

39 ETHI, *Témoignages*, 1^{re} session, 42^e législature, 2 octobre 2018, 1105 (Elizabeth Dubois, professeure adjointe, Département de communication, Université d'Ottawa).



des dispositions législatives sur la transparence et la reddition de comptes en matière d'utilisation politique des données personnelles⁴⁰.

M^{me} Dubois a indiqué que ce ne sont pas uniquement les partis politiques qui devraient faire l'objet de lois relatives à la protection des renseignements personnels, car ils ne sont pas les seuls à recueillir certaines données. Selon elle, puisque les organismes à but non lucratif, les syndicats et d'autres tierces parties font aussi une collecte de donnée similaire à celle que font les partis politiques « nous ne pouvons pas limiter l'examen de la collecte et de l'utilisation des données aux partis politiques en général »⁴¹.

Michael Pal, professeur agrégé en common law de la Faculté de droit de l'Université d'Ottawa, a de son côté souligné que bien que le projet de loi C-76, qui vise à modifier la *Loi électorale du Canada*, est « la mesure la plus importante que l'on ait prise pour exiger que les partis politiques protègent la vie privée », il ne va pas assez loin. Il ne donne pas de pouvoir au commissaire fédéral à la protection de la vie privée, il ne fixe pas un contenu précis devant être inséré dans les politiques sur la protection de la vie privée que les partis politiques doivent publier, et il ne prévoit pas de mécanisme d'application de la loi⁴².

M. Pal a noté que dans l'élaboration de la réglementation des partis politiques pour protéger la vie privée des électeurs « il faudra adapter le contenu des règles en vigueur au contexte particulier des partis politiques et des élections »⁴³.

Il a aussi encouragé les membres du Comité à voir la réglementation relative à la protection des renseignements personnels comme étant à l'avantage des partis politiques. Il a reconnu qu'être réglementé est souvent perçu comme étant onéreux et dispendieux, mais a invité les membres du Comité à imaginer « ce qui se passerait si l'un des principaux partis politiques du Canada était victime de piratage ». Selon M. Pal, il faudrait peu d'actes de piratage ou de cas de fuite de renseignements personnels détenus par un parti politique pour que le public perde confiance dans ce parti ou l'ensemble du système⁴⁴.

40 *Ibid.*

41 *Ibid.*

42 *Ibid.*, 1110 (Michael Pal, professeur agrégé, Faculté de droit, section de common law, Université d'Ottawa).

43 *Ibid.*

44 *Ibid.*, 1150.

Point de vue des partis politiques

Devant le Comité, le Parti libéral du Canada (« PLC »), le Parti conservateur du Canada (« PCC ») et le Nouveau parti démocratique du Canada (« NPD ») ont souligné leur engagement envers la protection des renseignements personnels. Ils ont confirmé que leur parti :

- A adopté une politique relative à la protection des renseignements personnels qui doit être suivie par tous les bénévoles, employés du parti et les sous-traitants, le cas échéant⁴⁵;
- Ne vend, ne loue ni ne partage les renseignements personnels qu'il détient sur les électeurs avec des tierces parties⁴⁶;
- Possède une base de données segmentée afin de s'assurer que ses bénévoles ou employés n'aient accès qu'à l'information dont ils ont besoin pour accomplir leurs tâches⁴⁷.
- Utilise des systèmes de cybersécurité afin de protéger les renseignements personnels qu'ils détiennent⁴⁸;
- Outre celles provenant d'InfoCanada ou de Poste Canada (annuaire et confirmation des adresses postales), n'achète pas de données⁴⁹; et
- Offre de la formation à tous les niveaux de leur organisation en matière de protection des renseignements personnels⁵⁰.

En ce qui concerne l'application des lois relatives à la protection des renseignements personnels aux partis politiques, l'opinion des partis varient.

45 ETHI, *Témoignages*, 1^{re} session, 42^e législature, 30 octobre 2018, 1100, 1105, 1110, 1115, 1120, 1140 (Trevor Bailey, agent de la protection de la vie privée et directeur des adhésions, Parti conservateur du Canada; Michael Fenrick, conseiller juridique et constitutionnel, Conseil national d'administration, Parti libéral du Canada; Jesse Calvert, directeur des opérations, Nouveau Parti démocratique).

46 *Ibid.*, 1100, 1145, 1200 (Trevor Bailey); *Ibid.*, 1105, 1145 et 1200 (Michael Fenrick); *Ibid.*, 1145 et 1200 (Jesse Calvert).

47 *Ibid.*, 1120 (Trevor Bailey); *Ibid.*, 1110 et 1125 (Michael Fenrick), *Ibid.*, 1115 et 1125 (Jesse Calvert).

48 *Ibid.*, 1100 et 1120 (Trevor Bailey); *Ibid.*, 1105 et 1125 (Michael Fenrick), *Ibid.*, 1115 et 1125 (Jesse Calvert).

49 *Ibid.*, 1135 (Trevor Bailey, Michael Fenrick and Jesse Calvert).

50 *Ibid.*, 1210 (Trevor Bailey, Michael Fenrick and Jesse Calvert); *Ibid.*, 1215 (Michael Fenrick and Jesse Calvert).



Michael Fenrick, conseiller juridique et constitutionnel du Conseil national d'administration du PLC, a rappelé que l'utilisation responsable des données peut contribuer à augmenter de façon importante la participation et la mobilisation à l'égard de notre processus politique et que les intérêts des partis politiques diffèrent de ceux d'entreprises commerciales. Selon lui « [c]e serait vraiment une désincitation réelle à la participation ou au processus politique si les gens pouvaient être exposés aux types de sanctions qui existent pour les sociétés, par exemple, en cas de non-respect de la LPRPDE »⁵¹. Le PLC n'appuie pas l'application de la LPRPDE aux partis politiques dans sa forme actuelle, car « elle vise à réguler l'activité commerciale, non pas l'activité politique »⁵².

Trevor Bailey, agent de la protection de la vie privée et directeur des adhésions du PCC, a indiqué que le PCC exerce ses activités en fonction de sa politique de protection de la vie privée, qui en ce moment, ne lui permet pas de se conformer entièrement à la LPRPDE. Il n'a pas voulu se prononcer sur la décision d'assujettir les partis politiques aux lois relatives à la protection des renseignements personnels ni sur la question de savoir s'il faut confier au commissaire à la protection de la vie privée un pouvoir de surveillance des activités des partis politiques⁵³. Cependant, il a indiqué que « si de nouvelles règles quant à la façon dont nous devons exercer nos activités sont présentées et entrent en vigueur », le PCC s'y conformerait, mais que cela requerrait « des consultations importantes, en plus de l'élaboration ou de la redéfinition de nos processus »⁵⁴.

Jesse Calvert, directeur des opérations du NPD a affirmé sans équivoque que le gouvernement du Canada devrait étendre l'application de la LPRPDE aux partis politiques. Il a indiqué que le NPD croit que les Canadiens méritent d'avoir confiance en leurs partis politiques et que la transparence est la seule façon de renforcer cette confiance. Il estime qu'il faut, dans un premier temps, que tous les partis politiques respectent les mêmes règles, et dans un deuxième temps, qu'il soit possible d'effectuer une surveillance de l'application des politiques internes de ces partis⁵⁵.

51 *Ibid.*, 1130 (Michael Fenrick).

52 *Ibid.*, 1215 (Michael Fenrick).

53 *Ibid.*, 1130 (Trevor Bailey).

54 *Ibid.*, 1130 et 1215 (Trevor Bailey).

55 *Ibid.*, 1135 (Jesse Calvert).

Point de vue du directeur général des élections

Le directeur général des élections, Stéphane Perrault, a indiqué son appui à la recommandation du Comité dans son rapport provisoire visant à ce que les partis politiques soient assujettis aux règles de base en matière de protection de la vie privée⁵⁶. Il a indiqué qu'à son avis, bien que le projet de loi C-76 obligerait les partis à publier leur politique de protection des renseignements personnels, il souffre de trois lacunes : il ne prévoit aucune norme minimale relative à la protection des renseignements personnels; il ne prévoit aucune surveillance par un organisme indépendant ; et il ne dit pas si les partis politiques devraient offrir aux Canadiens un mécanisme leur permettant de vérifier et de corriger toute information qu'un parti politique détient sur eux⁵⁷.

M. Perrault reconnaît que la capacité des partis politiques d'avoir accès à l'information qui leur permet de joindre les électeurs est un aspect fondamental de notre système électoral. Cependant, il demeure d'avis que des mesures de surveillance sont requises à l'égard des renseignements personnels qu'ils collectent et utilisent. Il estime qu'il y a moyen d'adapter les principes de la protection de la vie privée, par exemple au niveau des aspects du consentement et la façon dont il est obtenu, à la situation unique des partis politiques⁵⁸.

M. Perrault estime par ailleurs que le commissaire à la protection de la vie privée est la personne indiquée pour exercer une telle surveillance. Il croit aussi que les politiques de protection des renseignements personnels qui devront être publiées par les partis en vertu de la *Loi électorale du Canada* si le projet de loi C-76 est adopté devraient faire l'objet d'une surveillance du commissaire à la protection de la vie privée⁵⁹.

Point de vue du commissaire à la protection de la vie privée

La commissaire à l'information du Royaume-Uni a récemment présenté un rapport au Parlement dans le cadre de son enquête sur l'utilisation d'analyse de données dans les campagnes politiques. Dans ce rapport, elle rapporte que ses enquêteurs ont mené des entrevues auprès des onze principaux partis politiques au Royaume-Uni afin de réviser leurs pratiques en matière de collecte et d'utilisation de données personnelles. Les

56 ETHI, *Témoignages*, 1^{re} session, 42^e législature, 1^{er} novembre 2018, 1135 (Stéphane Perrault, directeur général des élections, Élections Canada).

57 *Ibid.*

58 *Ibid.*, 1145.

59 *Ibid.*, 1210.



enquêteurs ont aussi obtenu des partis de l'information à l'égard des mesures qu'ils prennent pour respecter les lois relatives à la protection des données. À la suite de l'enquête, la commissaire a conclu qu'il y avait des risques à l'égard du traitement des données personnelles par les partis politiques. Elle a émis des lettres d'avertissements dans lesquelles elle a demandé aux partis qu'ils soumettent une analyse d'impact relative à la protection des données pour leurs projets impliquant l'utilisation de données personnelles. Les partis doivent faire un suivi auprès du Commissariat à l'intérieur de trois mois. Ils ont aussi été avisés qu'ils feront l'objet d'un audit en janvier 2019⁶⁰.

Rien de ce qui précède ne peut être fait au Canada. Le CPVP est complètement dépourvu de pouvoirs de surveillance à l'égard des pratiques des partis politiques en matière de protection des renseignements personnels.

M. Therrien a comparu devant le Comité, le 1^{er} novembre 2018. Il a noté qu'un récent sondage mené par son organisation démontre que 92% des Canadiens souhaitent que les partis politiques soient assujettis aux lois relatives à la protection des renseignements personnels. Il a rappelé qu'en septembre 2018, les commissaires à la protection de la vie privée partout au Canada ont présenté une résolution conjointe qui exhorte les gouvernements à s'assurer que les partis politiques soient assujettis aux lois relatives à la protection des renseignements personnels. Il a affirmé que les experts universitaires, la société civile, le public canadien et le directeur général des élections sont tous d'accord avec leur position. Pourtant, le gouvernement a soutenu que la question méritait d'être étudiée, mais que les élections fédérales pouvaient se dérouler sans de telles mesures législatives⁶¹. Selon M. Therrien :

Le manque de surveillance exercée sur les pratiques de traitement des renseignements personnels des partis politiques canadiens devient malheureusement une exception par rapport aux autres pays et expose les élections canadiennes à une manipulation et à une utilisation non autorisée des renseignements personnels.

En d'autres termes, sans une réglementation appropriée des données, il y a un risque sérieux d'injustice dans le processus électoral lors des prochaines élections fédérales au Canada⁶².

En réponse à l'argument présenté par le PLC quant à l'effet dissuasif qu'aurait l'application de la LPRPDE sur les partis politiques en raison des pénalités qui peuvent être imposées, M. Therrien s'est dit surpris. Il explique que bien qu'il y ait des pénalités

60 *Investigation into the use of data analytics in political campaigns A report to Parliament*, pp. 23-24.

61 ETHI, *Témoignages*, 1^{re} session, 42^e législature, 1^{er} novembre 2018, 1120 (Daniel Therrien, commissaire à la protection de la vie privée)

62 *Ibid.*, 1220.

pour certains comportements spécifiques, y compris, depuis le 1^{er} novembre 2018, le fait de ne pas avoir divulgué les violations qui se sont produites, en règle générale « la LPRPDE souffre d'un manque d'application⁶³».

M. Therrien a rajouté qu'à sa connaissance « il n'a pas été démontré là où ces lois s'appliquent, et je n'ai pas vu de preuve [...] que la qualité de la communication serait compromise si les partis politiques étaient assujettis aux lois sur la protection de la vie privée⁶⁴ ». Il a aussi fait remarquer que si la LPRPDE s'appliquait aux partis politiques, il n'hésiterait pas à tenir compte du contexte dans lequel ils exercent leurs activités.

Premièrement, lorsque je recommande que la LPRPDE s'applique aux partis politiques fédéraux, il est implicite que le contexte serait important. La LPRPDE comporte un certain nombre de principes, comme le droit d'accès à l'information et le droit d'être clair quant aux fins auxquelles l'information serait utilisée par une entité assujettie à la LPRPDE. Le fait que nous ayons affaire à des partis politiques qui ont des intérêts légitimes, voire des droits, de participer à des discussions politiques avec les électeurs ferait partie du contexte.

Lorsque nous étudierons l'application de la LPRPDE aux partis politiques, nous pourrions certainement examiner les mécanismes d'application, le montant des sanctions et ce qui serait logique pour les diverses entités qui y sont assujetties⁶⁵.

Il a toutefois noté qu'en Colombie-Britannique, les mécanismes d'application sont les mêmes pour toutes les entités assujetties à la *Personal Information Protection Act*. Il a aussi rappelé que le RGPD et la loi en Colombie-Britannique s'appliquent aux partis politiques malgré le contexte particulier de leurs activités⁶⁶. Enfin, il a confirmé qu'à sa connaissance, aucune juridiction n'a créé de loi distincte pour réglementer les partis politiques⁶⁷. Pour M. Therrien le temps de l'autoréglementation est révolu.

Le gouvernement ne peut plus attendre pour agir. En l'absence d'une réforme globale, le Parlement devrait veiller à ce que des lois pertinentes sur la protection de la vie privée s'appliquent aux partis politiques. Il devrait également donner à mon bureau les mêmes pouvoirs d'inspection et d'application de la loi que ceux dont jouissent la plupart des partenaires commerciaux du Canada⁶⁸.

63 *Ibid.*, 1230.

64 *Ibid.*, 1245.

65 *Ibid.*, 1230.

66 *Ibid.*

67 *Ibid.*

68 *Ibid.*, 1220.



Enfin, comme M^{me} Dubois, M. Therrien a exprimé l'opinion que ce ne sont pas uniquement les partis politiques qui devraient être assujettis à l'application des lois relatives à la protection des renseignements personnels, mais plutôt « l'ensemble des organismes engagés dans des activités, commerciales ou non, qui colligent, utilisent ou transmettent des renseignements personnels », ce qui inclut les organismes à but non lucratif et les tiers⁶⁹.

Le Comité est d'avis que la confiance des citoyens canadiens serait mieux servie si les lois relatives à la protection des renseignements personnels s'appliquaient aux partis politiques et aux tierces parties politiques (telles que définies à l'article 349 de la *Loi électorale du Canada*). À la lumière des témoignages entendus, il réitère sa recommandation préliminaire à ce sujet, la recommandation 8 du rapport provisoire (recommandation 26 du présent rapport), et propose une nouvelle recommandation plus pointue en ce qui concerne les partis politiques. Le Comité réitère aussi la recommandation 5 de son rapport provisoire (recommandation 23 du présent rapport), qui vise l'octroi de pouvoirs d'audit additionnels au commissaire à la protection de la vie privée. Enfin, le Comité fait de nouvelles recommandations à l'égard des tierces parties politiques.

Recommandation 1 sur l'application des lois relatives aux renseignements personnels aux partis politiques :

Que le gouvernement du Canada modifie la *Loi sur la protection des renseignements personnels et les documents électroniques* pour y assujettir les partis politiques tout en tenant compte de leurs obligations de mener des activités d'information et de sensibilisation démocratique.

Recommandation 2 sur l'application des lois relatives aux renseignements personnels aux tierces parties politiques :

Que le gouvernement du Canada modifie la *Loi sur la protection des renseignements personnels et les documents électroniques* pour y assujettir les tierces parties politiques.

Recommandation 3 sur le pouvoir de surveillance en matière de protection des renseignements personnels des partis politiques et des tierces parties politiques :

Que le gouvernement du Canada octroie le mandat et l'autorité au commissaire à la protection de la vie privée ou à Élections Canada de mener des audits proactifs des partis politiques et des tierces parties politiques à l'égard de leurs pratiques relatives à la

69 *Ibid.*, 1255.

protection des renseignements personnels et d'émettre des ordonnances et des sanctions monétaires.

Recommandation 4 sur les ressources financières du Commissariat à la protection de la vie privée :

Que le gouvernement du Canada fournisse les ressources additionnelles nécessaires au Commissariat à la protection de la vie privée afin qu'il puisse faire face aux problèmes modernes liés à la protection de la vie privée et exercer de façon efficace les pouvoirs additionnels octroyés au commissaire.

UTILISATION DE FONDS ÉTRANGERS DANS LES ÉLECTIONS CANADIENNES

Vivian Krause, chercheuse et rédactrice, a soulevé des problèmes quant à l'utilisation de fonds étrangers pour financer le militantisme environnemental et électoral au Canada. Selon elle, la Direction des organismes de bienfaisance de l'Agence du Revenu du Canada (ARC) n'applique pas la *Loi de l'impôt sur le revenu* comme il se doit en matière d'enregistrement d'organismes de bienfaisance⁷⁰. Elle a offert quelques exemples d'organisations américaines qui auraient aidé à financer et orienter les activités d'organismes de bienfaisance canadiens actifs dans le cadre des élections fédérales de 2015. Selon elle, certaines de ces organisations sont des organismes de bienfaisance fictifs servant simplement à « canadianiser » des fonds⁷¹.

Selon M^{me} Krause, le projet de loi C-76 cherche à empêcher l'entrée de toutes devises étrangères, mais n'empêche pas la « canadianisation » de fonds⁷². À son avis, la meilleure façon de protéger les élections dépend donc de la volonté de l'ARC.

M. Perrault a indiqué ce qui suit à l'égard des préoccupations relatives au financement provenant de l'étranger:

Le projet de loi C-76 élargirait considérablement le régime actuel qui régit les tiers et inclurait diverses mesures visant à éliminer la possibilité d'utiliser des fonds provenant de l'étranger lors des élections canadiennes. Ces mesures comprennent en

70 ETHI, *Témoignages*, 1^{re} session, 42^e législature, 16 octobre 2018, 1130 (Vivian Krause, chercheuse et rédactrice).

71 ETHI, *Témoignages*, 1^{re} session, 42^e législature, 16 octobre 2018, 1135 (Vivian Krause).

72 *Ibid.*, 1255.



outre une clause anti-évitement et une interdiction de vendre de l'espace publicitaire à des entités étrangères⁷³.

M. Perrault a souligné que le projet de loi C-76 s'attaque à deux faiblesses de la *Loi électorale du Canada*.

La première est que dans le passé, les contributions se faisaient six mois avant la période électorale. De la façon dont la loi est rédigée, elles étaient traitées comme appartenant à l'entité: il s'agit de ses propres ressources, même si elles proviennent de l'étranger. La deuxième faiblesse, c'est que la loi actuelle réglemente la publicité électorale, qui est une catégorie de dépenses bien définie.

...

Le projet de loi C-76 nous fait avancer sur les deux fronts en étendant le champ des dépenses à toutes les activités partisans et en exigeant la déclaration de toutes les contributions. Il prévoit aussi des mesures supplémentaires. L'une d'elles, que j'ai recommandée au Comité, est l'adoption d'une clause anti-évitement qui vise précisément le genre de situation où l'argent passe d'une entité à une autre et où la source première se perd en cours de route⁷⁴.

Quant à la communication entre l'ARC et Élections Canada, M. Perrault a rappelé que ces questions relèveraient plutôt du commissaire aux élections fédérales⁷⁵.

L'une des organisations visées par les commentaires de M^{me} Krause lors de son témoignage est Tides Canada. Andrew Heitzman, le président du conseil d'administration de Tides Canada, a répondu aux allégations portées à l'égard de son organisation par M^{me} Krause. Dans une lettre au Comité, il insiste sur le fait que Tides Foundation aux États-Unis et Tides Canada sont deux organisations séparées. Il rajoute les explications suivantes :

Selon Mme Krause, Tides Canada était mêlée dans l'octroi de dons à des organismes sans vocation de bienfaisance à des fins notamment politiques. Ces allégations infondées et diffamatoires semblent reposer sur un manque de connaissance ou de pures faussetés à l'égard du cadre juridique des oeuvres de bienfaisance du Canada. Tides Canada ne verse aucune subvention à des organismes sans vocation de bienfaisance pour quelque raison que ce soit. Elle n'a jamais appuyé directement ou indirectement, par des subventions ou tout autre moyen, un parti politique, un politicien ou un candidat à une charge publique.

73 ETHI, *Témoignages*, 1^{re} session, 42^e législature, 1^{er} novembre 2018, 1130 (Stéphane Perrault).

74 *Ibid.*, 1150.

75 *Ibid.*, 1155.

Mme Krause continue à dresser un portrait erroné des travaux de Tides Canada et sur les renseignements qu'elle rend publics sur ses activités. Il s'agit d'une organisation bien respectée et gérée de façon professionnelle; elle se conforme en tout point aux lois et aux politiques canadiennes qui régissent les organismes de bienfaisance. D'ailleurs, l'Agence du revenu du Canada a procédé à un audit de la Fondation Tides Canada en 2016, et cette dernière demeure un organisme de bienfaisance enregistré en règle auprès de l'Agence. Tides Canada est en outre accréditée par le Programme de normes de l'organisme Imagine Canada, qui reconnaît l'excellence en matière de gouvernance, d'obligation redditionnelle et de transparence des organismes de bienfaisance⁷⁶.

Le Comité convient que le gouvernement du Canada devrait s'assurer que des fonds étrangers ne soient pas utilisés pour influencer les élections canadiennes et fait la recommandation qui suit.

Recommandation 5 sur le financement d'activités politiques par des fonds étrangers :

Que le gouvernement du Canada prenne toutes les mesures nécessaires afin de prévenir le financement étranger et l'influence étrangère dans les élections au Canada, y compris le financement étranger provenant d'organismes de bienfaisance enregistrés⁷⁷.

76 Lettre aux membres du Comité de la part d'Andrew Heintzman, président du conseil d'administration de Tides Canada, 15 novembre 2018. [TRADUCTION]

77 Le projet de loi C-76 est présentement étudié par le Sénat et pourrait régler la question s'il est adopté dans sa forme actuelle.

CHAPITRE 4 : RÉGLEMENTATION DES PLATEFORMES DE MÉDIAS SOCIAUX À L'ÈRE DE LA DÉSINFORMATION ET DE LA MÉSINFORMATION

CONTRE LA PROPAGATION DE DÉSINFORMATION ET DE MÉSINFORMATION EN LIGNE

Le Comité a entendu plusieurs témoignages soulevant des failles au niveau des plateformes de médias sociaux qui permettent ou facilitent la propagation de désinformation et de mésinformation. Le Comité a cerné trois éléments importants à considérer : la nature de l'écosystème d'information numérique, la structure même des plateformes de médias sociaux et les problèmes liés à l'autoréglementation.

Transformation de l'écosystème d'information

Loin est l'époque où le seul moyen pour les gens de s'informer était d'écouter la radio, de lire la copie d'un journal imprimé ou de regarder un bulletin de nouvelles en direct. Aujourd'hui, une quantité énorme de contenu se trouve en ligne et les éditeurs d'autrefois sont remplacés par l'intelligence artificielle (« IA »).

Taylor Owen, professeur agrégé en médias numériques et affaires mondiales à la University of British Columbia explique que jusqu'à l'émergence du Web social et du déclin des médias traditionnels, la responsabilité du discours acceptable était confiée à un petit nombre d'institutions médiatiques du XX^e siècle qui « maintenaient un système économique, et vraisemblablement un système politique, dont bénéficiaient certains groupes⁷⁸ ». Notre discours était donc limité et nous n'entendions pas les opinions de tous comme aujourd'hui. Lorsque le Web social est apparu, le débat dans la sphère publique est devenu plus « diversifié, dynamique et informatif que celui qui était restreint par l'infrastructure des médias traditionnels⁷⁹ ».

78 ETHI, *Témoignages*, 1^{re} session, 42^e législature, 25 septembre 2018, 1130 (Taylor Owen, professeur agrégé, Médias numériques et affaires mondiales, University of British Columbia).

79 *Ibid.*



Cependant, avec l'évolution des médias sociaux dans les dernières années, nous avons maintenant une nouvelle structure qui détermine ce qui est acceptable et définit les paramètres du débat public : le mécanisme de filtrage des plateformes qui détermine ce que nous voyons et si notre contenu peut être affiché. Selon M. Owen, nous devrions être préoccupés par le filtrage par algorithmes et les modèles d'affaires qui déterminent le contenu que nous voyons⁸⁰.

Ben Scott, directeur des politiques et de la défense des intérêts chez Omidyar Network, a comparé l'achat d'une revue chez un marchand de journaux dans un aéroport où le consommateur voit l'éventail de revues qu'il peut acheter dans divers secteurs (revue politique, de jardinage, de sports, etc.), à la consommation d'information en ligne, afin d'illustrer la différence entre les médias traditionnels et l'environnement numérique⁸¹.

Dans l'environnement numérique, tous ces secteurs sont regroupés dans un même endroit et tout se ressemble. C'est un fil d'actualités sur Facebook. C'est un fil de nouvelles sur Twitter. C'est une liste de vidéos sur YouTube. Dans cet environnement, tous les signes à propos de la crédibilité et de la qualité des sources que nous avions autrefois commencent à s'atténuer.

...

Nous avons perdu la structure normative qui, dans l'ancien univers médiatique, nous permettait en tant que citoyens de porter des jugements implicites à propos de la crédibilité des sources et, lorsque nous lisons les médias numériques, de faire preuve d'esprit critique⁸².

M^{me} Dubois a aussi soulevé un autre problème lié au nouvel écosystème d'information : l'évolution du système médiatique fait en sorte qu'auparavant répandre de la désinformation coûtait beaucoup plus cher et nécessitait beaucoup plus de ressources, alors que maintenant c'est facile de le faire⁸³.

À l'écosystème d'information s'ajoute le fait que les plateformes de médias sociaux ont des problèmes structurels intrinsèques.

80 *Ibid.*

81 ETHI, *Témoignages*, 1^{re} session, 42^e législature, 25 septembre 2018, 1125 (Ben Scott, directeur, Politiques et défense des intérêts, Omidyar Network).

82 *Ibid.*

83 ETHI, *Témoignages*, 1^{re} session, 42^e législature, 2 octobre 2018, 1200 (Elizabeth Dubois)

Problèmes structurels des plateformes de médias sociaux

M. Owen croit que la nature des vulnérabilités qui ont été révélées par l'atteinte à la sécurité n'est pas liée à des acteurs malveillants isolés, mais plutôt « aux problèmes structurels de notre infrastructure numérique qui [...] créent des vulnérabilités au sein de notre société libre et ouverte⁸⁴ ». Il a expliqué que nous nous trouvons maintenant dans l'ère des plateformes, où l'Internet est contrôlé par un petit nombre de sociétés propriétaires de plateformes d'information mondiales. Or, l'Internet des plateformes comporte deux problèmes structurels intrinsèques : la monétisation des plateformes, que l'on surnomme économie de l'attention, et le fait que le caractère de l'écosystème numérique et l'expérience des utilisateurs sont de plus en plus déterminés « par des systèmes d'intelligence artificielle qu'on ne peut tenir responsables⁸⁵ ».

Selon M. Owen, la monétisation des plateformes requiert une commercialisation de notre attention et de nos changements de comportement.

[L]es algorithmes des plateformes priorisent le divertissement, les informations-chocs et la radicalisation au détriment des informations fiables. Cela fait partie intégrante du modèle d'affaires. C'est d'ailleurs pour cette raison que la recherche démontre que les fausses nouvelles se répandent beaucoup plus largement et rapidement que les nouvelles authentiques⁸⁶.

En ce qui a trait à l'IA utilisée pour « filtrer le contenu, présenter le contenu le plus captivant, savoir ce qui suscite notre indignation et notre mobilisation, déterminer ce que voit l'utilisateur et déceler notre visibilité sur ces plateformes », M. Owen indique qu'elle sert à créer diverses versions de la réalité ciblées sur chacun d'entre nous que l'on peut appeler « hypercontrefaçons » ou « faux médias »⁸⁷.

M. Owen explique que les problèmes structurels des plateformes de médias sociaux sont responsables des externalités négatives que l'on observe dans la démocratie⁸⁸. Parmi ces externalités négatives, on retrouve la fragmentation et la vulnérabilité du processus électoral. M. Owen explique que chaque utilisateur se fait servir un menu d'information conçu sur mesure pour renforcer et cristalliser ses opinions. Une telle fragmentation « peut entraîner l'émergence fulgurante de la polarisation et du tribalisme » et « l'augmentation du nombre d'incidents de violence individuelle et collective dans le

84 ETHI, *Témoignages*, 1^{re} session, 42^e législature, 25 septembre 2018, 1100 (Taylor Owen).

85 *Ibid.*

86 *Ibid.*, 1100.

87 *Ibid.*

88 *Ibid.*, 1105.



monde réel »⁸⁹. En ce qui a trait à la vulnérabilité du processus électoral, il indique que des acteurs nationaux étrangers peuvent utiliser les leviers de l'économie de l'attention pour influencer le comportement des électeurs (p. ex. microciblage, cyberattaques, piratage informatique)⁹⁰.

M. Scott a qualifié de « cocktail toxique » la « politique du ressentiment que l'on observe dans le populisme contemporain et le pouvoir déformant du marché de l'information numérique⁹¹ ». M. McKelvey a noté que les algorithmes ne sont pas toujours efficaces pour déceler des renseignements de qualité ou crédibles. Le triage des renseignements a adopté une approche axée sur le marché, plutôt que sur la qualité du contenu⁹². Claire Wardle, présidente exécutive de First Draft, un organisme à but non lucratif sous la responsabilité du Shorenstein Center on Media Politics and Public Policy de la Kennedy School de l'Université Harvard, a indiqué que les gens cherchent de l'information, la consomment et la partagent en fonction de leurs émotions et a confirmé que cela est reflété par les algorithmes à l'œuvre sur les plateformes de médias sociaux. Plus il y a d'engagement envers un contenu, plus il risque de devenir viral. Le problème : le contenu trompeur est souvent celui qui crée la plus forte réaction et qui est mis en valeur⁹³.

Tristan Harris, cofondateur et directeur général du Center for Humane Technology, croit que la technologie n'est plus conçue pour s'adapter aux capacités de l'humain. Elle crée plutôt une distorsion qui commence à déformer et briser notre conception de la réalité. Selon M. Harris, en raison du fait que les gens regardent sans cesse leurs appareils électroniques chaque jour, leurs pensées sont maintenant générées par ce qu'elles voient sur des écrans, et cela représente une forme d'influence psychologique⁹⁴. L'auto-optimalisation des systèmes d'IA permet d'utiliser des algorithmes pour prédire le meilleur contenu à proposer à quelqu'un et la personnalisation des comptes d'utilisateurs permet de fournir à des milliards de gens des formes personnalisées de manipulation. À son avis, les entreprises technologiques ont un choix éthique à faire : revoir la conception de leurs produits et réaligner la façon dont la technologie

89 *Ibid.*

90 *Ibid.*

91 ETHI, *Témoignages*, 1^{re} session, 42^e législature, 25 septembre 2018, 1120 (Ben Scott)

92 *Ibid.*, 1205 (Fenwick McKelvey).

93 ETHI, *Témoignages*, 1^{re} session, 42^e législature, 16 octobre 2018, 1105 et 1140 (Claire Wardle, chercheuse associée, Shorenstein Center on Media, Politics and Public Policy, Kennedy School, Harvard University).

94 *Ibid.*, 1120 (Tristan Harris, cofondateur et directeur général, Center for Humane Technology).

fonctionne en tenant compte des limites de la capacité de l'humain à trouver un sens réel et à faire des choix, ou ne pas le faire et en subir les conséquences⁹⁵.

M. Harris soutient que la manipulation des plateformes de médias sociaux peut avoir des effets néfastes. Par exemple, elle peut avoir un effet nocif sur les enfants qui consomment du contenu en ligne. Contrairement aux médias traditionnels, qui font l'objet de réglementation (p. ex. interdiction de présenter certains programmes le samedi matin ou délai de cinq secondes) il n'y aucun filtre en ligne. Comme le souligne M. Harris :

[L]orsque les ingénieurs de Snapchat ou d'Instagram — qui, en passant, créent les applications les plus populaires pour les enfants — vont travailler chaque jour, ce sont des personnes de 20 à 30 ans, surtout des hommes, surtout des ingénieurs, des personnes versées dans les sciences informatiques ou formées dans la conception, et ils ne vont pas au travail chaque jour en se demandant comment protéger le développement identitaire des enfants [...] La seule chose qu'ils font, c'est travailler et se demander: « comment pouvons-nous les garder accrochés? Présentons cette chose appelée le "bouton Suivre", et maintenant ces enfants pourront se suivre l'un l'autre. Nous les avons tous branchés sur des fils de marionnettes, et ils sont occupés à se suivre l'un l'autre toute la journée, parce que nous voulons seulement qu'ils participent⁹⁶.

M. Harris explique que pour les plateformes de médias sociaux, à mesure que la compétition dans l'économie de l'attention s'intensifie, ce n'est plus suffisant qu'un utilisateur fasse le choix d'utiliser le produit – il faut maintenant entrer dans le tronc cérébral et le rendre dépendant, c'est-à-dire créer une habitude inconsciente⁹⁷. Le modèle d'affaires des sociétés de données consiste à accumuler le plus de renseignements personnels possible sur leurs utilisateurs et les manipuler. Il n'y a donc pas d'échange équitable entre les deux parties⁹⁸. Il note par exemple que YouTube n'aurait pas besoin de suggérer du contenu à droite de l'écran. Elle le fait parce que son modèle d'affaires vise la maximisation de la participation sur la plateforme. Le problème découle surtout du modèle d'affaires reposant sur la participation financée par la publicité⁹⁹.

M. Harris indique qu'il faut se demander à quel moment un éditeur est responsable de l'information qu'il transmet. Il estime logique que les entreprises technologiques ne

95 *Ibid.*, 1125.

96 *Ibid.*, 1155.

97 *Ibid.*, 1200.

98 *Ibid.*, 1220.

99 *Ibid.*, 1215 and 1230.



soient pas responsables de la quantité industrielle de contenu que les gens déversent sur leurs plateformes. Cependant, lorsque le contenu est alimenté par des recommandations générées par la plateforme à l'aide d'IA qu'elle a programmée (p. ex. vidéos d'Alex Jones recommandées 15 milliards de fois sur YouTube), il faut se demander si elles sont responsables d'avoir publié la recommandation¹⁰⁰. En les rendant responsables de leur modèle d'affaires, ce modèle devient plus coûteux.

À l'heure actuelle, nous avons des entreprises de technologie à combustion polluante qui utilisent ce modèle d'affaires pervers qui pollue le tissu social. Comme pour le charbon, nous devons faire en sorte que cette utilisation coûte plus cher. Vous payez donc pour les coûts externes qui apparaissent dans le bilan de la société, que ce soit la polarisation, la désinformation, la pollution épistémique, les problèmes de santé mentale, la solitude ou l'aliénation. Cela doit figurer dans les bilans des entreprises¹⁰¹.

M^{me} Dubois semble du même avis que M. Harris. Selon elle, il y a une distinction importante à faire entre « permettre l'existence de ce contenu » et « être responsable de ce que le contenu fait apparaître comme des sujets tendance, des résultats de recherche recommandés ou de l'information qui figure en haut des fils de nouvelles des gens¹⁰² ». Les plateformes prennent des décisions à l'égard de ce qui est mis en vedette et de ce qui ne l'est pas. Ces décisions devraient être prises en se demandant si elles réduisent au silence des groupes qui devraient pouvoir s'exprimer ou font la promotion de contenu qui ne devrait pas être publié ou mis en valeur¹⁰³.

Les problèmes structurels inhérents des plateformes de médias sociaux servent à alimenter l'économie de l'attention et à aider à la promotion de désinformation et de mésinformation envers des millions d'utilisateurs dépendants. Le Comité se préoccupe grandement des externalités négatives que causent ces plateformes.

Insuffisance de l'autoréglementation

Le commissaire à la protection de la vie privée a utilisé un ton alarmant pour décrire la situation actuelle.

La semaine dernière, j'ai assisté à la 40e Conférence internationale des commissaires à la protection des données et de la vie privée, à Bruxelles. La conférence a confirmé ce que j'avais expliqué dans mon dernier rapport annuel, à savoir qu'il y a une crise dans le

100 *Ibid.*, 1205.

101 *Ibid.*, 1230.

102 ETHI, *Témoignages*, 1^{re} session, 42^e législature, 2 octobre 2018, 1145 (Elizabeth Dubois)

103 *Ibid.*

domaine de la collecte et du traitement des renseignements personnels en ligne. Même les géants de la technologie [...] reconnaissent que le statu quo ne peut pas continuer.

Le PDG d'Apple, Tim Cook, a parlé d'un « complexe industriel de données » et a averti que « nos propres renseignements, des plus banals aux plus personnels, sont utilisés contre nous comme des armes avec une efficacité militaire ». [...] Mark Zuckerberg, de Facebook, a admis que son entreprise avait commis un grave abus de confiance dans l'affaire Cambridge Analytica. Les deux entreprises se sont montrées favorables à une nouvelle loi américaine semblable au Règlement général sur la protection des données de l'Union européenne, le RGPD.

Lorsque les géants de la technologie deviennent de fervents partisans d'une réglementation contraignante, il apparaît évident que la situation a changé et que nous vivons effectivement une crise.

...

Le gouvernement est toutefois lent à agir, mettant ainsi en péril la confiance des Canadiens envers l'économie numérique, nos processus démocratiques et nos autres valeurs fondamentales ¹⁰⁴.

M. Therrien a également rappelé l'importance de la protection de la vie privée :

La protection de la vie privée n'est pas un droit que nous sacrifions simplement au profit de l'innovation, de l'efficacité ou des gains commerciaux. Nul n'a librement consenti à ce que ses renseignements personnels soient utilisés comme arme contre lui [...]. De même, nous ne pouvons permettre que le processus démocratique canadien soit perturbé, pas plus que nous ne pouvons accepter que nos institutions soient minées dans la course à la numérisation tous azimuts simplement parce que la technologie rend cela possible¹⁰⁵.

M. Owen a indiqué que lorsque des externalités négatives sont créées par des monopoles qui sont très peu réglementés, les gouvernements doivent intervenir pour protéger l'intérêt collectif¹⁰⁶. À son avis, une démarche stratégique globale visant la réforme des mécanismes de réglementations des plateformes de médias sociaux et notre relation avec l'économie numérique est nécessaire¹⁰⁷.

M. Scott est aussi d'avis qu'il ne faut pas compter sur le secteur privé pour régler le problème puisque les « monopoles cotés en bourse ne s'autoréglementent pas ». Selon

104 ETHI, *Témoignages*, 1^{re} session, 42^e législature, 1^{er} novembre 2018, 1215 (Daniel Therrien).

105 *Ibid.*, 1220.

106 ETHI, *Témoignages*, 1^{re} session, 42^e législature, 25 septembre 2018, 1110 (Taylor Owen).

107 *Ibid.*, 1110.



lui il faut que le gouvernement « utilise ses outils pour réorienter le marché vers l'intérêt public ». Il suggère par exemple l'adoption d'une charte numérique de la démocratie, qui énoncerait un ensemble de principes et établirait des politiques claires permettant d'entreprendre les changements nécessaires pour protéger l'intégrité de notre sphère publique démocratique¹⁰⁸.

M^{me} Dubois a indiqué que l'autoréglementation est inefficace dans le cas des grandes plateformes. Elle estime qu'il faut tenir ces entreprises responsables du contenu qu'elles affichent sur leurs plateformes et veiller à ce que la manipulation qu'elles font des données qu'elles détiennent soit transparente et responsable. Elle a expliqué qu'à l'heure actuelle, on se heurte à une « boîte noire », car « [n]ous ne savons pas comment les sociétés Facebook et Google décident de ce qu'elles permettent ou non que l'on affiche dans leurs plateformes »¹⁰⁹. Elle a rajouté une raison importante pour laquelle il est important que le Canada réglemente les plateformes de médias sociaux : la majorité des plateformes de médias sociaux sont de grandes entreprises internationales qui ne connaissent pas nécessairement les particularités de la population canadiennes lorsqu'elles conçoivent leur autoréglementation¹¹⁰.

Risques liés à la réglementation

Malgré ce qui précède, certains témoins ont soulevé des réserves à l'égard de la réglementation des plateformes de médias sociaux.

Par exemple, Colin McKay, chef des politiques publiques et des relations gouvernementales chez Google Canada, malgré qu'il ait confirmé que Google a pris les mesures nécessaires pour se conformer au RGDP, a souligné que « le prolongement du RGPD créerait de plus grandes obligations en matière de conformité pour les petites et moyennes entreprises » qui ressentent déjà partout dans le monde « le stress lié au fait de comprendre leurs obligations en vertu du RGPD¹¹¹ ». À l'égard de la possibilité que des vérificateurs indépendants débarquent chez Google pour vérifier la bonne utilisation de leurs algorithmes, il a indiqué : « [d]ans certains cas, l'algorithme est une technologie commerciale exclusive, et je ne sais pas si un vérificateur aurait la capacité d'évaluer ce

108 *Ibid.*, 1120 (Ben Scott).

109 ETHI, *Témoignages*, 1^{re} session, 42^e législature, 2 octobre 2018, 1105 (Elizabeth Dubois).

110 *Ibid.*, 1235.

111 ETHI, *Témoignages*, 1^{re} session, 42^e législature, 23 octobre 2018, 1205 et 1215 (Colin McKay, chef, Politiques publiques et relations gouvernementales, Google Canada)

que l'algorithme est censé faire ni de quelle façon il évaluerait ce qui fonctionne ou ce qui ne fonctionne pas, et d'après quelle norme¹¹² ».

En ce qui concerne la possibilité de mettre en place un organisme public indépendant qui assurerait l'administration et la prise de décision relative au droit à l'oubli et la protection des renseignements personnels en matière de diffamation, de harcèlement ou de discours haineux (plutôt que de laisser les plateformes le faire), M. McKay a soulevé le possible conflit avec la liberté d'expression que le retrait de contenu peut entraîner. Selon lui, la meilleure solution est de faire appel aux tribunaux qui comprennent à la fois les normes et les attentes du public. Il a semblé douter de la légitimité de l'idée de donner la responsabilité de déterminer des questions liées à la liberté d'expression à un tribunal administratif¹¹³.

Oath Inc. (« Oath »), une filiale de Verizon qui comprend plusieurs plateformes numériques, dont AOL, Yahoo et Tumblr, a soumis un mémoire au Comité. Elle y discute de ses pratiques, puis indique qu'elle soutient l'autoréglementation de l'industrie. Elle convient que l'autoréglementation n'est pas la panacée de la protection de la vie privée, mais estime qu'elle assure un écosystème de conformité coopérative. Elle supporte l'autoréglementation de l'industrie en matière de publicité numérique, par exemple en vertu de l'Alliance de la publicité numérique du Canada¹¹⁴.

Samantha Bradshaw, une chercheuse qui participe au projet de recherche sur la propagande numérique du Oxford Internet Institute, a aussi exprimé une crainte à l'égard de la réglementation excessive et le risque qu'une réglementation qui force le retrait d'un certain contenu sur les plateformes de médias sociaux puisse mener à la perte d'une partie importante du débat démocratique¹¹⁵. M. Pal a fait écho à ses commentaires, indiquant que « nous voulons faciliter l'expression politique et non la restreindre. Certaines des lois qui pourraient être adoptées pourraient restreindre l'expression politique¹¹⁶ ».

Le Comité tient compte des commentaires des représentants de l'industrie et de certains universitaires, mais estime néanmoins qu'une forme de réglementation est requise.

112 *Ibid.*, 1245.

113 *Ibid.*, 1250.

114 Oath Inc., *Mémoire*, p.6.

115 ETHI, *Témoignages*, 1^{re} session, 42^e législature, 2 octobre 2018, 1125 (Samantha Bradshaw, chercheuse).

116 *Ibid.*, 1145 (Michael Pal).



SOLUTIONS RÉGLEMENTAIRES POTENTIELLES

Transparence en matière de publicité en ligne

Plusieurs témoins ont discuté du besoin de plus de transparence en matière de publicité qu'on retrouve sur les plateformes de médias sociaux. Par exemple, M. Scott a soutenu qu'il n'y a « aucune raison pourquoi un citoyen qui voit une publicité politique ne devrait pas savoir exactement qui l'a achetée, combien il a dépensé et combien de personnes ont été payées pour acheter l'annonce¹¹⁷ ». À son avis, il faudrait aussi qu'un électeur sache pourquoi il reçoit un message afin d'examiner la publicité politique d'un œil plus critique¹¹⁸. Il suggère qu'il devrait y avoir une petite boîte qui s'ouvre lorsqu'un individu passe le curseur de son appareil électronique sur une publicité en ligne et donne de l'information sur la publicité telle « qui a acheté la publicité; combien elle a coûté; combien de gens l'ont vue à part vous; et surtout, les raisons pour lesquelles vous avez eu cette publicité, soit les caractéristiques démographiques qui ont été choisies par l'annonceur pour que vous voyiez cette annonce¹¹⁹ ».

M. Scott a également suggéré que « toutes les annonces à saveur politique qu'il y a sur Facebook, Twitter ou Google devraient se trouver dans une base de données accessible au public », qui permet au public de voir quel genre de messages sont envoyés à divers publics cibles et si ces messages diffèrent selon l'auditoire¹²⁰. Cette base de données devrait être accessible aux journalistes et chercheurs et avoir une interface simple donnant un accès facile aux données, permettant d'examiner les publicités et de comprendre comment la propagande politique fonctionne¹²¹. Certaines entreprises ont annoncé qu'elles allaient créer des bases de données axées sur la transparence, mais selon M. Scott les bases de données ne correspondent pas aux normes recherchées. À son avis, il faudra légiférer pour atteindre cette norme¹²².

L'autre difficulté, selon M. Scott, est la définition de « publicité politique » qui n'est pas toujours la même selon la plateforme¹²³. M^{me} Wardle a abondé dans le même sens,

117 ETHI, *Témoignages*, 1^{re} session, 42^e législature, 25 septembre 2018, 1125 (Ben Scott).

118 *Ibid.*

119 *Ibid.*, 1150.

120 *Ibid.*

121 *Ibid.*

122 *Ibid.*, 1155.

123 *Ibid.*

soulignant l'importance de ne pas trop restreindre ce que l'on considère une publicité de nature politique :

Si tout type de politique ou même de règlement s'applique simplement aux publicités qui mentionnent un candidat ou le nom d'un parti, nous passerons à côté du moteur de toute campagne de désinformation, c'est-à-dire les messages visant à accentuer les clivages actuels dans la société en ce qui concerne l'ethnicité, la religion, la race, la sexualité, le sexe et la classe sociale ainsi que des enjeux sociaux précis [...] ¹²⁴.

Elle supporte la création d'une base de données centrale et ouverte des publicités politiques en format lisible et en temps réel ¹²⁵.

M. Pal a indiqué qu'il serait bon de créer un dépôt public de toutes les publicités liées aux élections. Il a reconnu que Facebook l'a récemment fait volontairement, mais que la société pourrait changer d'avis à tout moment. Il faudrait donc que ce dépôt soit exigé par la loi ¹²⁶. Il a aussi souligné que la *Loi électorale du Canada* et les lois connexes régissent les partis politiques, les candidats à la direction, les candidats à l'investiture et les partis tiers, mais qu'il faudrait ajouter les plateformes de médias sociaux et les entreprises de technologie aux groupes qui sont explicitement réglementés par ces lois. Ces plateformes devraient être responsables de divulguer et de tenir des dossiers sur la source de toute entité qui cherche à y afficher sa publicité de nature politique ¹²⁷.

M. Perrault a précisé que le projet de loi C-76 obligerait les plateformes de médias sociaux à publier et à conserver un registre des publicités électorales et partisans, appuyant ainsi la transparence. Il clarifierait et élargirait aussi les dispositions actuelles qui visent certaines formes d'usurpation d'identité en ligne et certaines fausses déclarations concernant les candidats ¹²⁸.

De son côté, M. Owen croit en une transparence complète qui ne se limite pas aux publicités politiques. Il estime que comme consommateur dans un contexte de protection du consommateur ou comme électeur dans un contexte de protection de l'intégrité du processus électoral, nous devrions avoir le droit de savoir comment nous

124 ETHI, *Témoignages*, 1^{re} session, 42^e législature, 16 octobre 2018, 1105 (Claire Wardle).

125 *Ibid.*, 1105, 1140.

126 ETHI, *Témoignages*, 1^{re} session, 42^e législature, 2 octobre 2018, 1115 (Michael Pal).

127 *Ibid.*, 1110.

128 ETHI, *Témoignages*, 1^{re} session, 42^e législature, 1^{er} novembre 2018, 1130 (Stéphane Perrault).



sommes ciblés par certaines informations « de façon très précise à l'aide de systèmes incroyablement sophistiqués dans le but d'influencer notre comportement¹²⁹ ».

En matière de transparence de publicités en ligne, le Comité reconnaît que le projet de loi C-76 devrait apporter plusieurs mesures importantes, en obligeant notamment les plateformes de médias sociaux à publier et à conserver un registre des publicités électorales et partisans. Cependant, certains témoignages semblent confirmer que les bases de données mises sur pied par les plateformes de médias sociaux ne sont pas suffisamment faciles à utiliser ou aisément consultables. Le Comité recommande donc ce qui suit comme mesure additionnelle à ce qui est déjà prévu dans le projet de loi C-76 :

Recommandation 6 sur la publicité politique :

Que le gouvernement du Canada modifie la *Loi électorale du Canada* pour obliger un mandataire à soumettre une pièce d'identité et une preuve d'adresse lors de la mise en ligne de publicités politiques.

Recommandation 7 sur la création d'une base de données de publicités politiques en ligne :

Que le gouvernement du Canada modifie la *Loi électorale du Canada* pour obliger les plateformes de médias sociaux à s'assurer que les bases de données consultables et lisibles par machine de publicités politiques en ligne qu'elles créent soient faciles à naviguer et permettent à quiconque de trouver des publicités à l'aide de filtres tels que : la personne qui a financé l'annonce, la question politique couverte, la période pendant laquelle l'annonce était en ligne, et la démographie du public cible.

Le Comité réitère également la recommandation 1 de son rapport provisoire relative à la transparence (recommandation 19 du présent rapport).

Transparence des algorithmes et responsabilité à l'égard du contenu

M. Scott estime que nous devons examiner comment les algorithmes utilisés par les plateformes de médias sociaux fonctionnent et leur incidence sur le bien-être social. Nous devons comprendre les faiblesses qui font en sorte qu'ils puissent être utilisés comme arme afin d'être en mesure d'éviter ces effets négatifs importants¹³⁰. De son

129 ETHI, *Témoignages*, 1^{re} session, 42^e législature, 25 septembre 2018, 1200 (Taylor Owen).

130 *Ibid.*, 1125 et 1135 (Ben Scott).

côté, M. Owen a donné l'exemple d'une loi récemment adoptée en Californie qui forcera, à partir de juin 2019, tous les comptes automatisés à s'auto-identifier comme étant automatisés¹³¹. Il reconnaît qu'il y a « toutes sortes d'utilisations positives potentielles des robots et des outils automatisés dans l'écosystème social ». Cependant, il estime qu'en tant que consommateurs, nous devrions être en mesure de savoir si nous sommes ciblés par l'un de ces robots¹³².

M^{me} Dubois a suggéré ce qui suit à l'égard de la transparence algorithmique.

Par exemple, on pourrait appliquer des processus d'essai plus clairs qui permettent aux gouvernements ou aux universitaires de vérifier les procédures. On pourrait vérifier régulièrement les algorithmes tout comme on audite des données financières. On pourrait exiger que l'équipe documente son élaboration des algorithmes, sa prise de décisions et qu'elle explique ces décisions. Il faut aussi étiqueter plus clairement les comptes automatisés dans les médias sociaux et dans les applications de messagerie instantanée et enregistrer les communications numériques automatisées avec les électeurs. On pourrait modifier le registre de communication avec les électeurs pour y inclure les contacts numériques automatisés¹³³.

Elle a rajouté qu'il serait bon de pouvoir consulter un historique des décisions que l'équipe qui crée un algorithme a prises en l'élaborant. De cette façon, on pourrait apprendre ce que l'algorithme était censé faire, pourquoi et comment¹³⁴.

M^{me} Bradshaw a quant à elle souligné que s'il était possible d'examiner les principes qui sous-tendent la conception algorithmique (p. ex. le caractère viral de l'information) et de les remplacer par des principes appuyant une meilleure démocratie, par exemple « les principes sur l'information factuelle provenant de médias professionnels plutôt que des sources qui produisent constamment des nouvelles trompeuses ou bidon, il serait possible de réglementer les plateformes sans nuire à la liberté d'expression ». Elle suggère par exemple que les médias professionnels devraient peut-être avoir une priorité dans les algorithmes¹³⁵.

131 *Ibid.*, 1135 (Taylor Owen).

132 *Ibid.*

133 ETHI, *Témoignages*, 1^{re} session, 42^e législature, 2 octobre 2018, 1105 (Elizabeth Dubois).

134 *Ibid.*

135 *Ibid.*, 1225 (Samantha Bradshaw).



M^{me} Wardle a elle aussi souligné le besoin de plus de transparence en ce qui concerne le comportement des plateformes de médias sociaux et des décisions qui sont prises par celles-ci, par exemple en matière d'automatisation du contenu¹³⁶.

À la lumière de ces témoignages, le Comité fait les recommandations suivantes en matière de transparence algorithmique et de responsabilité des plateformes de médias sociaux envers le contenu publié en ligne :

Recommandation 8 sur la réglementation de certaines plateformes de médias sociaux :

Que le gouvernement du Canada adopte une loi visant à réglementer les plateformes de médias sociaux en utilisant comme modèle les seuils de portée au Canada décrits au paragraphe 325.1(1) du projet de loi C-76, Loi modifiant la Loi électorale du Canada et d'autres lois et apportant des modifications corrélatives à d'autres textes législatifs. Parmi ces responsabilités, devrait être inclus un devoir :

- d'étiqueter clairement le contenu produit automatiquement ou algorithmiquement (p.ex. par des « robots ») ;
- de détecter et supprimer les comptes non authentiques et frauduleux qui se font passer pour d'autres pour des raisons malveillantes ;
- de respecter un code de pratique qui interdirait les pratiques trompeuses ou injustes et qui exigerait une réponse rapide aux signalements de harcèlement, de menaces et de discours haineux, et l'obligation de retirer le contenu diffamatoire, frauduleux et manipulé à des fins malveillantes (p. ex. les vidéos contrefait appelés « deep fake ») ; et
- d'étiqueter clairement la publicité politique ou autre publicité payante.

Recommandation 9 sur la transparence algorithmique :

Que le gouvernement du Canada édicte des exigences en matière de transparence en ce qui concerne les algorithmes et fournisse à un organisme de réglementation existant ou nouveau le mandat et l'autorité de faire des vérifications d'algorithmes.

136 ETHI, [*Témoignages*](#), 1^{re} session, 42^e législature, 16 octobre 2018, 1215 (Claire Wardle).

Le Comité souhaite préciser que les sanctions monétaires imposées en vertu des nouvelles mesures législatives proposées devraient excéder le seul coût de faire des affaires pour une entreprise.

Modération du contenu

M. Scott a indiqué que les citoyens devraient avoir le droit d'être protégés contre le contenu illégal. Le discours incitant à la haine, les propos diffamatoires, ceux qui équivalent à du harcèlement ou incitent à la violence sont tous considérés comme illégaux hors ligne. Selon lui, un tel contenu devrait aussi être considéré comme illégal en ligne et retiré rapidement des plateformes des médias sociaux au moyen d'un « processus rigoureusement supervisé par un contrôle judiciaire régulier assorti d'un processus d'appel afin de veiller à ne pas compromettre la liberté d'expression ». Il estime que le pouvoir de retirer le contenu illégal ne doit pas être cédé aux plateformes de médias sociaux, mais que leur participation est nécessaire afin d'accélérer le processus¹³⁷.

M^{me} Bradshaw a aussi discuté de modération de contenu, donnant comme exemple le cas du Myanmar et la façon dont Facebook a été utilisé pour propager de la désinformation qui a mené à de la violence à l'égard du peuple Rohingya, la minorité islamique de ce pays. Ce cas illustre selon elle le fait que les plateformes de médias sociaux opèrent à une échelle mondiale, mais n'ont pas nécessairement du personnel sensible aux réalités de chaque pays pour assurer la modération du contenu à l'égard de problèmes locaux. Elle encourage une modération de contenu plus mondiale et inclusive afin d'éviter que ce soit un modérateur de contenu situé en Californie qui prenne des décisions sur le contenu de pays où il y a, par exemple, des tensions ethniques¹³⁸.

Recommandation 10 sur le retrait de contenu illégal par les plateformes de médias sociaux :

Que le gouvernement du Canada introduise une loi imposant une obligation aux plateformes de médias sociaux de retirer, dans un délai raisonnable, le contenu manifestement illégal qui s'y retrouve, incluant le discours incitant à la haine, le harcèlement et la désinformation, sous peine de faire face à une sanction monétaire imposée en fonction d'une échelle de responsabilité proportionnelle à la dominance et à l'importance de la plateforme sociale et qui prévoit une supervision judiciaire du retrait de contenu et un droit d'appel.

137 ETHI, *Témoignages*, 1^{re} session, 42^e législature, 25 septembre 2018, 1125 (Ben Scott).

138 ETHI, *Témoignages*, 1^{re} session, 42^e législature, 2 octobre 2018, 1230 (Samantha Bradshaw).



Contrôle et consentement de l'utilisateur

M. Scott a soulevé des dispositions du RGPD pour discuter de l'importance du consentement. Une disposition du RGPD empêche maintenant les ententes de confidentialité qui ne donnent pas aux gens des choix réels en matière de contrôle de leurs propres données. Ainsi, les ententes de confidentialité comme celle proposée par Facebook, où il s'agit de tout ou de rien (si j'accepte de signer l'entente, je peux accéder à une plateforme utilisée par deux milliards de personnes; si je ne la signe pas, je renonce à tous les services de Facebook) ne sont plus permises. De l'avis de M. Scott, il faut donner aux consommateurs une plus grande capacité de contrôle à l'égard des données qui sont recueillies à leur sujet et la façon dont elles sont utilisées. Pour M. Owen, certains principes, dont celui du consentement et le fait d'être informé, représentent des protections contre la mauvaise utilisation de ces renseignements personnels.

Si nous consentons régulièrement à l'utilisation, au partage et à l'intégration de nos données personnelles — si nous avons droit à ce consentement — et si nous avons le droit de savoir comment ces données sont utilisées, que ce soit pour établir des profils psychographiques, pour mener une campagne de microciblage dirigée par une intelligence artificielle ou pour d'autres raisons, cela nous protège et nous immunise contre le risque potentiel posé par ces technologies à l'avenir, et non contre la façon dont elles ont été utilisées à un certain moment par un certain groupe¹³⁹.

M. Therrien a souligné qu'une nouvelle législation canadienne devrait accorder une place importante au consentement valable, mais aussi tenir compte d'autres moyens de protéger la vie privée lorsque l'obtention du consentement n'est pas réaliste, par exemple dans le développement de l'intelligence artificielle. À cet égard, il a noté que le concept d'intérêt légitime du RGPD pourrait être envisagé¹⁴⁰.

Le Comité réitère la recommandation 2 de son rapport provisoire, qui vise l'implantation de mesures similaires à celles contenues dans le RGPD (recommandation 20 du présent rapport).

139 ETHI, [Témoignages](#), 1^{re} session, 42^e législature, 25 septembre 2018, 1215 (Taylor Owen).

140 ETHI, [Témoignages](#), 1^{re} session, 42^e législature, 1^{er} novembre 2018, 1220 (Daniel Therrien).

CHAPITRE 5 : UN RÉGULATEUR INDÉPENDANT?

Devant le Comité, M. Therrien a indiqué que toute nouvelle législation visant la réglementation de la protection des renseignements personnels qui se retrouvent sur les plateformes de médias sociaux devrait être fondée sur les droits et rédigée comme une loi qui confère des droits, plutôt qu'un code de conduite pour l'industrie et qu'elle devrait permettre une innovation responsable. Il a suggéré que cette législation devrait aussi « habiliter une autorité publique », indiquant que ce pourrait être son bureau ou une autre autorité publique à émettre des lignes directrices contraignantes quant à l'application des principes généraux dans des circonstances précises¹⁴¹.

LES PLATEFORMES DE MÉDIAS SOCIAUX COMME DIFFUSEURS

Au cours de son étude, le Comité s'est demandé si les plateformes de médias sociaux devraient être traitées de la même façon que les radiodiffuseurs.

Michael Pal a soulevé cette possibilité en indiquant que si c'était le cas, lorsqu'une plateforme comme Facebook agirait comme un diffuseur elle serait assujettie aux mêmes obligations que les radiodiffuseurs en vertu de l'article 348 de la *Loi électorale du Canada*, qui exige que ces derniers facturent le tarif le plus bas possible aux partis politiques qui désirent placer de la publicité sur leurs plateformes et empêchent les responsables des radiodiffuseurs d'offrir des tarifs préférentiels aux partis politiques qu'ils préfèrent¹⁴². M. McKelvey s'est aussi demandé si les plateformes de médias sociaux devraient relever du CRTC puisque selon lui, elles « fonctionnent parfois précisément comme des diffuseurs et elles entrent dans une nouvelle catégorie à qui se pose le problème de modération des contenus »¹⁴³.

Scott Hutton, directeur exécutif de la radiodiffusion du CRTC, a confirmé que l'organisation pour laquelle il travaille assure un certain contrôle sur les émissions diffusées au Canada et effectue une modération sur le contenu. La *Loi sur la radiodiffusion* exige que toutes les émissions diffusées au Canada soient de haute qualité. En ce qui concerne le contenu, le CRTC travaille dans un régime de

141 ETHI, *Ibid.*

142 ETHI, *Témoignages*, 1^{re} session, 42^e législature, 2 octobre 2018, 1115 (Michael Pal).

143 ETHI, *Témoignages*, 1^{re} session, 42^e législature, 25 septembre 2018, 1230 (Fenwick McKelvey).



coréglementation. Il applique divers codes qui ont été élaborés au cours d'instances publiques avec les Canadiens et avec les radiodiffuseurs afin de maintenir un haut standard de qualité. Certaines dispositions dans les règlements qu'applique le CRTC indiquent comment traiter les sujets qui contreviennent à la loi, qui sont abusifs, qui faussent l'information ou qui visent à tromper¹⁴⁴.

M. Hutton a confirmé que le CRTC réglemente tant les grands diffuseurs que « les plus petits diffuseurs comme une radio ou télévision communautaire ou autochtone en milieu rural ou en région éloignée¹⁴⁵ ». Ainsi, une radio communautaire rejoignant quelques centaines de personnes doit s'astreindre à certaines règles en matière de diffusion et est assujettie à une surveillance réglementaire, alors qu'un compte Facebook qui diffuse du contenu à des millions de personnes échappe à ce genre de surveillance.

À la question de savoir si les plateformes de médias sociaux, qui se comportent de plus en plus comme des diffuseurs d'information, devraient être assujetties à la *Loi sur la radiodiffusion*, M. Hutton a répondu par l'affirmative, indiquant que « toute partie qui bénéficie de l'exploitation de la radiodiffusion au Canada devrait faire partie de notre système¹⁴⁶ ».

M. Hutton s'est référé au rapport interactif publié par le CRTC le 31 mai 2018 et intitulé *Emboîter le pas au changement: L'avenir de la distribution de la programmation au Canada* dans lequel le CRTC a indiqué que « l'approche réglementaire traditionnelle permet de moins en moins d'atteindre les objectifs énoncés dans des lois comme la *Loi sur la radiodiffusion* ». Le CRTC propose une approche novatrice en matière de politiques et de réglementation des plateformes numériques guidée par trois principes, dont :

Le deuxième principe est que toutes les parties qui tirent profit d'une participation au système de radiodiffusion devraient contribuer au système de manière appropriée et équitable. Les nouvelles politiques et les nouveaux règlements doivent tenir compte du fait que les responsabilités sociales et culturelles liées à l'exploitation au Canada s'appliquent aux plateformes numériques¹⁴⁷.

144 ETHI, *Témoignages*, 1^{re} session, 42^e législature, 1^{er} novembre 2018, 1210 (Scott Hutton, directeur exécutif, Radiodiffusion, Conseil de la radiodiffusion et des télécommunications canadiennes).

145 *Ibid.*

146 *Ibid.*, 1205.

147 *Ibid.*, 1140.

Le CRTC estime donc que toute partie qui bénéficie de l'exploitation du système de diffusion au Canada en assume les responsabilités sociales. Cela inclut les plateformes de médias sociaux¹⁴⁸.

NORMES CONCERNANT LA MODÉRATION DU CONTENU EN LIGNE

M. McKelvey a soulevé l'idée de créer un Conseil national des médias sociaux, qui serait semblable à un conseil des normes de la radiotélévision, « pour que vous puissiez commencer à coordonner cette zone grise associée à la modération du contenu, ce que les plateformes font de plus en plus¹⁴⁹ ».

Il a souligné les similarités que ce conseil pourrait avoir avec le CRTC :

Ce dernier conseil ressemble beaucoup à ce qui a été réclamé et à ce dont nous avons besoin en matière de modération des contenus. Il prévoit en effet un processus d'appel et il assure la transparence et la divulgation. Je dois concéder que ça relève davantage de l'autoréglementation de l'industrie. C'est une critique, mais c'est aussi une étape importante pour faire converger l'intérêt vers cette activité particulière qu'est la modération des contenus, à laquelle la loi n'a pas encore bien reconnu toute son importance¹⁵⁰.

Le Comité est d'avis que cette suggestion mérite considération.

148 *Ibid.*, 1210.

149 ETHI, *Témoignages*, 1^{re} session, 42^e législature, 25 septembre 2018, 1140 (Fenwick McKelvey).

150 *Ibid.*, 1235.

CHAPITRE 6 : RÉGLEMENTATION DU POUVOIR MONOPOLISTIQUE DES GÉANTS DE LA TECHNOLOGIE ET DU MONOPOLE DES DONNÉES

Depuis la publication de son rapport provisoire en juin 2018, le Comité s'est intéressé particulièrement à la question du monopole des données détenu par les géants de la technologie et à la nécessité d'assujettir ces derniers à un contrôle plus strict de leurs activités. Les témoignages de Maurice Stucke, du Bureau de la concurrence, de la Banque du Canada et des autres témoins cités dans ce chapitre ont nourri la réflexion du Comité à cet égard.

TÉMOIGNAGES PERTINENTS

Maurice Stucke

Maurice Stucke, qui est professeur de droit au College of Law de l'Université du Tennessee, a comparu devant le Comité le 4 octobre 2018. Il a publié en mars 2018 un article intitulé *Should We Be Concerned About Data-opolies?*¹⁵¹, qui est à l'origine de l'expression que le Comité a retenue pour décrire la situation de monopole des données détenu par quelques géants de la technologie (« data-opolies » en anglais).

Lors de sa comparution, M. Stucke a traité des risques d'une éventuelle monopolisation des données par quelques entreprises puissantes en abordant notamment la manière dont les responsables de la concurrence de l'Union européenne et des États-Unis les ont perçus et du risque de préjudice qu'ils représentent pour les consommateurs¹⁵².

M. Stucke a décrit les monopoles de données de la manière suivante :

Les monopoles de données contrôlent une plateforme clé à travers laquelle un volume important et une variété de données personnelles circulent. La vitesse d'acquisition et

151 Maurice E. Stucke, *Should We Be Concerned About Data-opolies?*, 19 mars 2018, 2 Georgetown Law Technology Review 275 (2018); University of Tennessee Legal Studies Research Paper No. 349.

152 ETHI, *Témoignages*, 1^{re} session, 42^e législature, 4 octobre 2018 1110 (Maurice Stucke, professeur, College of Law, University of Tennessee).



d'exploitation de ces données personnelles peut aider ces entreprises à obtenir un pouvoir important sur le marché¹⁵³.

Il a ensuite expliqué les huit méfaits potentiels des monopoles de données qu'il a identifiés :

- 1) la dégradation de la qualité
- 2) la surveillance
- 3) le transfert de richesse des consommateurs aux monopoles de données
- 4) la perte de confiance
- 5) l'imposition de coûts importants à des tiers
- 6) la diminution de l'innovation dans les marchés dominés par les monopoles de données
- 7) les préoccupations sociales et morales des monopoles de données
- 8) les visées politiques des monopoles de données¹⁵⁴.

En ce qui concerne le cinquième élément, l'imposition de coûts importants à des tiers, M. Stucke a fourni les précisions suivantes :

on parle de la relation entre ennemis ou frères ennemis que les monopoles de données ont avec les concepteurs d'applications. Ils ont besoin de ces développeurs d'applications pour attirer les utilisateurs sur leur plateforme, mais une fois qu'ils ont commencé à leur faire concurrence, ils peuvent les traiter en ennemis. Ils peuvent adopter diverses pratiques anticoncurrentielles, notamment en dégradant la fonctionnalité de l'application. Ce qui est particulièrement important pour vous, c'est que les monopoles de données peuvent imposer des coûts aux entreprises qui cherchent à protéger notre vie privée¹⁵⁵.

M. Stucke a inclus dans le septième élément, c'est-à-dire les préoccupations sociales et morales des monopoles de données, la préoccupation liée au fait que les monopoles de données créent intentionnellement une dépendance à leurs produits. Selon lui,

153 *Ibid.*

154 *Ibid.*

155 *Ibid.*, 1115.

Ici, il y a une interaction intéressante entre le monopole et la concurrence. Normalement, un monopoliste n'a pas à craindre que les consommateurs aillent ailleurs. Ici, cependant, il est profitable pour les trusts de données d'amener les utilisateurs à passer plus de temps sur leur plateforme. Ils peuvent ainsi obtenir plus de données, les cibler avec de la publicité et augmenter leurs profits¹⁵⁶.

Enfin, en ce qui concerne le huitième élément, les visées politiques des monopoles de données, M. Stucke a noté que le pouvoir économique se traduit souvent par un pouvoir politique et que les monopoles de données ont des outils que les monopoles précédents n'avaient pas, « c'est-à-dire la capacité d'influencer le débat public et notre perception du bien et du mal¹⁵⁷. »

M. Stucke a résumé la situation des monopoles de données dans les trois points suivants :

Pour commencer, les monopoles de données peuvent causer plus de torts que les autres monopoles. Ils peuvent toucher non seulement nos portefeuilles. Ils peuvent avoir une incidence sur notre vie privée, notre autonomie, notre démocratie et notre bien-être.

Deuxièmement, les marchés dominés par ces monopoles ne se corrigeront pas nécessairement d'eux-mêmes.

Troisièmement, l'application de la loi antitrust peut jouer un rôle clé, mais dans ce cas-ci, la loi antitrust est une condition nécessaire, mais non suffisante pour stimuler la concurrence en matière de protection de la vie privée. Il faut vraiment assurer la coordination avec les responsables de la protection de la vie privée et des consommateurs¹⁵⁸.

En réponse aux questions des membres du Comité, M. Stucke a fait remarquer que dans un marché concurrentiel, on pourrait penser que les consommateurs obtiennent des produits et des services adaptés à leur vie privée, mais que ce n'est pas le cas¹⁵⁹.

Il a également fait remarquer que les autorités responsables de la concurrence au Canada et aux États-Unis accordent beaucoup d'importance au facteur prix dans les fusions et qu'une application plus stricte des lois antitrust permettrait une meilleure

156 *Ibid.*

157 *Ibid.*

158 *Ibid.*, 1120.

159 *Ibid.*



évaluation des effets non liés aux prix, comme les fusions axées sur des données¹⁶⁰.

Selon M. Stucke,

Une solution serait une application plus éclairée des lois antitrust. C'est *ex post*. On aurait alors *ex ante*, des exigences semblables au RGPD qui pourraient aider à renforcer la protection de la vie privée. Pour les utilisateurs, le transfert des données s'en trouverait facilité. Une autre solution consisterait à donner plus de précision sur les détenteurs des données et sur les droits de propriété de chacun sur ses données personnelles¹⁶¹.

En ce qui concerne la portabilité des données – ou leur transférabilité – M. Stucke a attiré l'attention du Comité sur le fait que

[L]e RGPD contient certaines mesures qui semblent prometteuses, telle la transférabilité des données, et qui peuvent répondre à certaines préoccupations liées à la concurrence, mais il faut tenir compte du fait que la transférabilité des données n'est pas nécessairement utile lorsque la vitesse de propagation des données est en jeu. Voici un bon exemple: les applications de cartographie. Vous pouvez transporter vos données pour Google Maps, par exemple, mais cela ne sera pas utile pour une application de navigation qui doit savoir où vous êtes en ce moment même. Le fait de pouvoir reporter des données d'il y a six mois ne va pas permettre à cette nouvelle application de navigation de concurrencer Waze, qui appartient à Google, et Google Maps¹⁶².

Invité à formuler des recommandations sur la manière d'habiliter le Bureau de la concurrence à faire face à ces monopoles de données, M. Stucke a argué que cela pourrait se faire notamment en abandonnant les outils axés sur les prix lorsqu'il s'agit de marchés qui sont manifestement gratuits et d'utiliser plutôt une autre valeur, comme une diminution faible mais significative et non transitoire de la protection de la vie privée. De plus, M. Stucke a recommandé d'envisager une coordination entre l'autorité responsable de la protection de la vie privée et celle responsable de la concurrence. Il a aussi recommandé de se pencher sur les mesures d'exécution de la loi pour s'assurer qu'elles arrivent à dissuader les comportements répréhensibles¹⁶³.

M. Stucke a conclu son témoignage en arguant que « si l'on veut profiter des avantages d'une économie axée sur les données de sorte que cette économie soit inclusive, protège notre démocratie et puisse aussi protéger notre vie privée et améliorer notre bien-être », on doit revenir à l'idée que le gouvernement doit jouer un rôle clé dans la

160 *Ibid.*, 1125.

161 *Ibid.*

162 *Ibid.*, 1150.

163 *Ibid.*, 1230.

prestation de certains services essentiels qu'un marché, même concurrentiel, ne pourrait pas offrir¹⁶⁴.

Bureau de la concurrence

Le Bureau de la concurrence – sous la direction du commissaire de la concurrence – est responsable de l'administration et de l'application de la *Loi sur la concurrence* et de trois autres lois concernant l'étiquetage¹⁶⁵. Il est notamment responsable d'examiner les transactions de fusion – afin de s'assurer que la société amalgamée n'exerce pas un pouvoir indu sur le marché, au détriment des clients, des fournisseurs et des consommateurs canadiens – ainsi que les situations d'abus de position dominante.

Le 19 février 2018, le Bureau de la concurrence a publié un rapport intitulé *Mégadonnées et innovation : les grands thèmes de la politique en matière de concurrence au Canada*, qui constitue une synthèse des thèmes clés soulevés dans le cadre d'une consultation publique fondée sur un document de travail du Bureau (« *Mégadonnées et innovation : conséquences sur la politique en matière de concurrence au Canada* »). Dans ce rapport, le Bureau de la concurrence conclut notamment que, dans son état actuel, le droit de la concurrence canadien permet d'évaluer adéquatement les fusions d'entreprises et les pratiques monopolistiques dans le contexte des mégadonnées¹⁶⁶.

En ce qui concerne les plateformes basées sur les données (le rapport cite les exemples de Google, Uber et Amazon), le Bureau de la concurrence estime que

[l']idée la plus importante est que la nature d'une « transaction » ou d'un « prix » diffère selon qu'il s'agit d'une plateforme ou non. Par exemple, un prix « élevé » d'un côté d'une plateforme ne constitue pas forcément une preuve de puissance commerciale ou d'effets anticoncurrentiels, parce qu'il découle d'un prix « faible » d'un autre côté de la plateforme¹⁶⁷.

Le rapport aborde également la question des cartels. À cet égard, le Bureau de la concurrence est d'avis que l'arrivée des algorithmes informatiques qui font appel aux

164 *Ibid.*, 1245.

165 Il s'agit de la *Loi sur l'emballage et l'étiquetage des produits de consommation*, L.R.C. 1985, ch. C-38, de la *Loi sur l'étiquetage des textiles*, L.R.C. 1985, ch. T-10 et de la *Loi sur le poinçonnage des métaux précieux*, L.R.C. 1985, ch. P-19.

166 Bureau de la concurrence, *Mégadonnées et innovation : les grands thèmes de la politique en matière de concurrence au Canada*, 19 février 2018, p. 7.

167 *Ibid.*, p. 8.



mégadonnées ne devrait pas mener à repenser l'application du droit de la concurrence aux cartels¹⁶⁸. Le Bureau de la concurrence ajoute que, bien qu'il soit prématuré de suggérer un changement fondamental dans l'application des dispositions de la *Loi sur la concurrence* relatives aux cartels, ce dernier continuera à évaluer « d'autres éléments de preuve liés à cette question en développement¹⁶⁹ ».

En ce qui concerne la publicité, le Bureau de la concurrence note que son mandat, qui consiste à garantir la véracité des publicités, peut chevaucher le mandat du CPVP, qui consiste à protéger le droit à la vie privée¹⁷⁰. Selon le rapport,

[I]es deux mandats sont importants pour protéger les consommateurs dans l'économie numérique. Le Bureau continuera d'appliquer les dispositions de la Loi, même si les actes criminels en cause peuvent être sujets à une mesure d'exécution en vertu de la LPRPDE. Le Bureau partage l'opinion du Commissariat quant à l'importance de la collaboration dans ce domaine, et il sera heureux de travailler avec lui pour protéger les consommateurs canadiens¹⁷¹.

Le rapport fait ainsi référence au mémoire déposé par le CPVP dans le cadre des consultations publiques du Bureau de la concurrence, qui mentionne que

[I]e Commissariat serait donc ravi de discuter de la façon dont le Commissariat et le Bureau de la concurrence pourraient coopérer pour répondre à ces nouveaux défis. On viserait ainsi à aider les entreprises à mieux comprendre leurs obligations en matière de conformité afin d'assurer une meilleure protection et d'établir la confiance des particuliers à l'égard de l'économie numérique canadienne¹⁷².

En somme, le Bureau de la concurrence argue dans ce rapport que l'émergence d'entreprises qui contrôlent et exploitent les données peut donner lieu à de nouveaux défis en matière d'application du droit de la concurrence, « sans toutefois être en soi une source de préoccupation¹⁷³ ». Le Bureau de la concurrence conclut que même si « les mégadonnées peuvent comprendre des méthodes et des outils assez spécialisés et

168 *Ibid.*, p. 11.

169 *Ibid.*, p. 13.

170 *Ibid.*, p. 16.

171 *Ibid.*

172 *Ibid.*, faisant référence au mémoire du CPVP à l'intention du Bureau de la concurrence du 17 novembre 2017 intitulé « [Consultation sur le document de travail Mégadonnées et innovation](#) ».

173 *Ibid.*, p. 18.

moins bien connus », le cadre traditionnel de l'application du droit de la concurrence peut continuer d'orienter utilement ses activités¹⁷⁴.

Des représentants du Bureau de la concurrence ont comparu le 18 octobre 2018. Anthony Durocher, qui est sous-commissaire à la Direction des pratiques monopolistiques, a noté deux cas où la protection de la vie privée peut être pertinente pour le Bureau de la concurrence :

Premièrement, si des entreprises se livrent concurrence pour attirer de nouveaux utilisateurs en offrant une protection de la vie privée, cette dimension de la concurrence peut être un facteur pertinent dans l'examen des activités anticoncurrentielles. Deuxièmement, si une entreprise trompe des consommateurs quant au fait que leurs données seront utilisées ou à la façon dont elles le seront, une telle situation pourrait également soulever des préoccupations liées à la Loi sur la concurrence¹⁷⁵.

Il a également affirmé ce qui suit, par rapport aux préoccupations récurrentes concernant la taille et la croissance de certaines entreprises de technologie :

Grossir, c'est la récompense qu'une entreprise peut obtenir lorsqu'elle réussit à offrir un produit novateur. Nous ne devrions pas punir la réussite. C'est seulement lorsqu'on trouve des preuves qu'une grande entreprise s'adonne à un comportement anticoncurrentiel préjudiciable que nous devrions intervenir¹⁷⁶.

En ce qui concerne la concurrence à l'ère de l'économie numérique en général, M. Durocher a fait les commentaires suivants :

[D]ans l'économie numérique, nous sommes passés d'une concurrence statique à une concurrence dynamique. La concurrence statique, c'est la concurrence de l'ancien monde sur les prix et les extrants, laquelle occupe encore une place importante dans nombre d'industries partout au Canada. Dans le domaine numérique, ce que nous voyons, c'est que les entreprises se livrent une grande concurrence pour les utilisateurs en fonction de la façon dont elles innovent au chapitre de l'offre de leurs produits aux consommateurs. Nous appelons cela les effets non liés aux prix. Lorsque je parle de la modernisation des outils que nous utilisons dans le cadre de la Loi sur la concurrence, c'est exactement dans le but de régler ces problèmes d'effets non liés aux prix¹⁷⁷.

174 *Ibid.*

175 ETHI, *Témoignages*, 1^{re} session, 42^e législature, 18 octobre 2018, 1115 (Anthony Durocher, sous-commissaire, Direction des pratiques monopolistiques, Bureau de la concurrence).

176 ETHI, *Témoignages*, 1^{re} session, 42^e législature, 18 octobre 2018, 1120 (Anthony Durocher, sous-commissaire, Direction des pratiques monopolistiques, Bureau de la concurrence).

177 ETHI, *Témoignages*, 1^{re} session, 42^e législature, 18 octobre 2018, 1235 (Anthony Durocher, sous-commissaire, Direction des pratiques monopolistiques, Bureau de la concurrence).



Sur la question de la portabilité des données et de l'interopérabilité des systèmes, M. Durocher a offert le point de vue suivant :

La portabilité des données visée par le Règlement général sur la protection des données est l'aspect le plus notable, à mon avis, du point de vue de la concurrence. En théorie, elle peut favoriser la concurrence. Elle peut permettre aux consommateurs de transférer leurs données d'une plateforme à une autre. Évidemment, les difficultés surgissent des menus détails pour ce qui est de la façon dont cela est rendu opérationnel, mais c'est certainement quelque chose que nous prenons en note¹⁷⁸.

Banque du Canada

La Banque du Canada est la banque centrale du pays et son rôle principal, énoncé dans le préambule de la *Loi sur la Banque du Canada*, consiste à « favoriser la prospérité économique et financière du Canada ». Les quatre grandes sphères de responsabilité de la Banque sont la politique monétaire, le système financier, la monnaie et la gestion financière¹⁷⁹.

Le 8 février 2018, Carolyn A. Wilkins, qui est la première sous-gouverneure de la Banque du Canada, a prononcé un discours dans le cadre du Symposium du G7 sur l'innovation et la croissance inclusive (« [À la croisée des chemins : l'innovation et la croissance inclusive](#) »). Dans son discours, M^{me} Wilkins a abordé la question de certaines entreprises « phares » dans le domaine des technologies de l'information – en donnant les exemples des médias sociaux et des plateformes en ligne – qui bénéficient de la concentration du marché et dégagent d'énormes bénéfices de leur activité monopolistique. Selon M^{me} Wilkins,

[I]a nouveauté, c'est que cette impression selon laquelle le « gagnant rafle toute la mise » s'amplifie dans une économie numérique, car les données des utilisateurs y deviennent une autre source de monopole. Les données d'un grand réseau créent dès lors un obstacle considérable à l'entrée de concurrents sur le marché. Un autre obstacle peut résider dans la stratégie de certaines entreprises qui, étant en mesure de contrôler l'accès à des services en ligne essentiels, exploitent cette situation pour entraver leurs concurrents¹⁸⁰.

Par ailleurs, M^{me} Wilkins a reconnu l'apport du secteur des technologies à la bonne tenue de l'économie, tout en soulignant que la taille de certaines entreprises et leur

178 ETHI, *Témoignages*, 1^{re} session, 42^e législature, 18 octobre 2018, 1235 (Anthony Durocher, sous-commissaire, Direction des pratiques monopolistiques, Bureau de la concurrence).

179 Banque du Canada, *Au sujet de la Banque*.

180 Banque du Canada, « [À la croisée des chemins : l'innovation et la croissance inclusive](#) », p. 4.

domination du marché soulèvent des inquiétudes récurrentes concernant les effets potentiels du pouvoir monopolistique sur les prix et la concurrence¹⁸¹.

Les données constituent par ailleurs un nouveau facteur pour la domination d'un marché. Le fait d'avoir accès aux données des utilisateurs et de maîtriser ces données pourrait rendre certaines entreprises essentiellement inattaquables. Celles-ci peuvent aisément évincer la concurrence en conjuguant leur dimension et une utilisation novatrice des données pour anticiper et combler les besoins en constante évolution de leurs clients, et ce, à moindre coût (voire gratuitement). Cette situation a deux effets indésirables. Premièrement, les entreprises qui mènent leurs activités dans des environnements où la concurrence est moins féroce innovent moins. Nous avons besoin du dynamisme suscité par l'entrée de nouveaux acteurs sur le marché et de la contestabilité des marchés pour faire augmenter la croissance tendancielle le plus possible. Deuxièmement, les plus grosses entreprises pourraient très bien se remettre à fixer les prix de manière monopolistique à long terme. Ces conséquences font obstacle à une croissance plus forte et plus inclusive¹⁸².

La situation décrite a mené M^{me} Wilkins à recommander, en priorité, « de moderniser les politiques antitrust et sur la concurrence, de même que les législations appropriées¹⁸³ ». Selon elle, une réflexion doit avoir lieu quant au meilleur moyen d'éliminer les obstacles à l'entrée de nouveaux concurrents et sur la façon de réglementer la propriété et le partage des données des utilisateurs, qui « constituent la principale source des rentes de monopole à l'ère numérique¹⁸⁴ ». M^{me} Wilkins a d'ailleurs noté certaines idées intéressantes qui ont été avancées à cet égard, comme « la possibilité de donner aux utilisateurs la maîtrise de leurs données – voire d'obliger les entreprises à payer les utilisateurs pour les obtenir – et de réglementer les plateformes technologiques comme des services publics¹⁸⁵ ».

M^{me} Wilkins a conclu son discours en arguant que, de concert avec la formation de la main-d'œuvre et la gestion des risques opérationnels, « le contrôle de la puissance du marché, plus précisément de la puissance conférée par la maîtrise des données des consommateurs, pour favoriser la concurrence et limiter les bénéfices monopolistiques » est l'un des trois domaines où une meilleure stratégie pourrait être formulée et appliquée¹⁸⁶.

181 *Ibid.*

182 *Ibid.*, p. 6 et 7.

183 *Ibid.*, p. 7.

184 *Ibid.*

185 *Ibid.*

186 *Ibid.*, p. 9.



Un représentant de la Banque du Canada a comparu le 18 octobre 2018. Eric Santor, qui est directeur général des Analyses de l'économie canadienne, a ajouté ce qui suit à l'idée exprimée par M^{me} Wilkins – dans le discours mentionné précédemment – à l'effet qu'il existe une impression selon laquelle le gagnant rafle toute la mise dans une économie numérique parce que les données des utilisateurs deviennent une autre source de monopole :

Les données d'un grand réseau créent dès lors un obstacle considérable à l'entrée de concurrents sur le marché. Un autre obstacle peut résider dans la stratégie de certaines entreprises, qui étant en mesure de contrôler l'accès à des services en ligne essentiels, exploitent cette situation pour entraver leurs concurrents et freiner l'innovation. Dans ces circonstances, nous sommes d'avis que les politiques en matière de concurrence peuvent être adéquatement modernisées afin de veiller à ce que nous tirions pleinement parti de la numérisation¹⁸⁷.

En ce qui a trait à la question des entreprises « phares » évoquée par M^{me} Wilkins dans son discours, M. Santor a souligné : « [I]l y a une des préoccupations que suscite chez nous la domination des entreprises phares tient au fait que celles-ci disposent d'un pouvoir plus important quand il s'agit de fixer leurs prix, ce qui pourrait faire augmenter les prix »¹⁸⁸.

Ben Scott, Tristan Harris et Colin McKay

Selon Ben Scott, le moment est venu d'examiner la politique sur la concurrence en vigueur :

Nous devons envisager de moderniser la politique antitrust pour entraver les pratiques anti-concurrentielles, restreindre les fusions et les acquisitions et faciliter l'accès au marché pour de nouveaux types de services qui offrent des solutions de rechange aux modèles existants dont les facteurs externes ont donné lieu à des résultats négatifs¹⁸⁹.

Quant à Tristan Harris, il a résumé ainsi les défis qui se présentent en matière de concurrence et d'interopérabilité des systèmes¹⁹⁰ :

187 ETHI, *Témoignages*, 1^{re} session, 42^e législature, 18 octobre 2018, 1130 (Eric Santor, directeur général, Analyses de l'économie canadienne, Banque du Canada).

188 *Ibid.*

189 ETHI, *Témoignages*, 1^{re} session, 42^e législature, 25 septembre 2018, 1125 (Ben Scott, directeur, Politiques et défense des intérêts, Omidyar Network).

190 L'interopérabilité est « la capacité que possède un système, un logiciel ou une interface informatique à fonctionner avec d'autres, existants ou futurs, sans restriction d'accès ou de mise en œuvre, quelle que soit la langue, le lieu ou le logiciel en cause ». Voir : Laurence Bich-Carrière, « Propriété intellectuelle et

si vous essayez de mettre sur pied un substitut à Facebook, à YouTube ou à Twitter, ce serait très difficile pour vous d'y parvenir, parce que ces plateformes reposent sur les effets des réseaux.

...

On doit être en mesure de passer d'un réseau à l'autre de manière interopérable.

...

Je pense que nous devons envisager des choses semblables. Ce qui est plus difficile avec les réseaux sociaux, c'est que vous ne pouvez pas simplement déplacer vos données ailleurs, parce que celles-ci sont connectées à tous les messages que vous avez affichés dans les profils d'autres personnes et qu'elles sont protégées par des paramètres de confidentialité, vous ne pouvez donc pas simplement migrer vers une nouvelle plateforme. Je pense qu'il s'agit d'un domaine très important, et il a trait à la consolidation du pouvoir et à la capacité d'écraser la concurrence¹⁹¹.

Observant le problème par l'autre bout de la lorgnette, Colin McKay a mentionné un projet de Google pour faciliter le transfert de données entre différents services. Google a conçu ce projet sur lequel ses employés travaillent avec des partenaires de l'industrie et qui représente, selon M. McKay, « une solide tentative pour commencer à surmonter » la difficulté pratique que pose l'interopérabilité des systèmes¹⁹².

CONCLUSIONS ET RECOMMANDATIONS

À la lumière de ce qui précède, le Comité estime qu'à la recommandation faite dans son rapport provisoire de modifier la LPRPDE pour y ajouter une obligation de permettre la portabilité des données devrait s'ajouter une recommandation de modifier la LPRPDE pour y inclure l'obligation de rendre possible l'interopérabilité des systèmes afin de permettre le transfert des données d'une plateforme à l'autre.

Le Comité estime également que la *Loi sur la concurrence* devrait être mise à jour, notamment pour s'assurer que le Bureau de la concurrence prenne en compte dans ses évaluations les effets non liés aux prix, comme les fusions axées sur les données, et pour

émojis : 😊 ou 🤖? », dans *Développements récents en droit de la propriété intellectuelle*, vol. 449, Éditions Yvon Blais, Montréal, 2018, p. 314 et 315.

191 ETHI, *Témoignages*, 1^{re} session, 42^e législature, 16 octobre 2018, 1245 (Tristan Harris, directeur, Politiques et défense des intérêts, Omidyar Network).

192 ETHI, *Témoignages*, 1^{re} session, 42^e législature, 23 octobre 2018, 1140 et 1215 (Colin McKay, chef, Politiques publiques et relations gouvernementales, Google Canada).



établir un cadre permettant au Bureau de la concurrence et au CPVP de collaborer lorsqu'il est approprié de le faire. Pour ces raisons, le Comité recommande :

Recommandation 11 sur la portabilité des données et l'interopérabilité des systèmes :

Que la *Loi sur la protection des renseignements personnels et les documents électroniques* soit modifiée en y ajoutant les principes relatifs à la portabilité des données et à l'interopérabilité des systèmes.

Recommandation 12 sur la modernisation de la *Loi sur la concurrence* :

Que le gouvernement du Canada étudie les dommages économiques potentiellement causés par les soi-disant « monopoles de données » au Canada et qu'il détermine si la modernisation de la *Loi sur la concurrence* est requise.

Ajoutant à sa recommandation préliminaire 7 sur le partage d'information entre le commissaire à la protection de la vie privée et d'autres organismes de régulation (recommandation 25 du présent rapport), le Comité recommande également :

Recommandation 13 sur la collaboration entre le Bureau de la concurrence et le Commissariat à la protection de la vie privée :

Que la *Loi sur la protection des renseignements personnels et les documents électroniques* et la *Loi sur la concurrence* soient modifiées afin d'établir un cadre permettant au Bureau de la concurrence et au Commissariat à la protection de la vie privée de collaborer lorsqu'il est approprié de le faire.

CHAPITRE 7: CYBERSÉCURITÉ

L'origine de la présente étude étant une atteinte à la sécurité de renseignements personnels dont Facebook avait la charge, le Comité s'est naturellement penché sur la question de la cybersécurité. Les témoignages des représentants du Centre de la sécurité des télécommunications, de Ben Scott, de Maurice Stucke, de Michael Pal et du directeur général des élections du Canada ont été particulièrement utiles au cours de cette réflexion.

TÉMOIGNAGES PERTINENTS

Centre de la sécurité des télécommunications

Selon le Centre de la sécurité des télécommunications (CST), il est le « centre canadien d'excellence en matière de cyberopérations ».

Le CST est l'un des principaux organismes de sécurité et de renseignement du Canada. Il protège les réseaux informatiques et les renseignements de grande importance du Canada et procède à la collecte de renseignement électromagnétique étranger. Le CST fournit également de l'assistance aux organismes chargés de l'application de la loi et de la sécurité dans leurs activités légalement autorisées lorsqu'ils requièrent l'expertise unique de l'organisme¹⁹³.

En 2017, en réponse à une demande de la ministre des Institutions démocratiques, le CST a mené une évaluation des cybermenaces contre le processus démocratique canadien, ciblant particulièrement les ordres de gouvernement fédéral, provincial, territorial et municipal en ce qui concerne les élections, les partis politiques et les politiciens, ainsi que les médias. Pour fonder son analyse, le CST a examiné les cybermenaces qui ont ciblé les processus démocratiques du Canada et d'autres pays dans le monde au cours des 10 dernières années. Le 16 juin 2017, le CST a publié un rapport intitulé [Cybermenaces contre le processus démocratique du Canada](#) dans lequel il résume les résultats de son évaluation.

Le rapport rappelle notamment qu'une cybermenace avait ciblé les élections fédérales de 2015 au Canada. En ce qui concerne les élections fédérales qui auront lieu en 2019, le CST s'attend à ce que « de nombreux groupes d'hacktivistes déploient des

193 Centre de la sécurité des télécommunications, [Cybermenaces contre le processus démocratique du Canada](#), 16 juin 2017, p. 3.



cybercapacités en vue d’influencer le processus démocratique » et à ce que « la majorité de ces activités seront de faible complexité, mais nous nous attendons à ce que certaines activités d’influence soient bien planifiées et ciblent plus d’un aspect du processus démocratique¹⁹⁴ ».

Fait à noter, le CST estime dans son rapport que « les partis politiques, les politiciens et les médias sont plus vulnérables aux cybermenaces et aux opérations d’influence que les activités entourant les élections à proprement parler¹⁹⁵ ». Ceci s’explique, selon le CST, « par le fait que le scrutin s’effectue avec des bulletins de vote en papier et par les mesures juridiques, procédurales et liées aux technologies de l’information mises en place par Élections Canada¹⁹⁶ ».

Le CST constate également qu’à l’échelle mondiale, les adversaires¹⁹⁷ du Canada ciblent les élections, les partis politiques et les politiciens, ainsi que les médias traditionnels et les médias sociaux en utilisant leurs cybercapacités :

- pour nuire aux élections en entravant la participation des électeurs, en trafiquant les résultats des élections et en volant les renseignements personnels des électeurs;
- contre les partis politiques et les politiciens en effectuant des activités de cyberespionnage à des fins de coercition, de manipulation et pour discréditer publiquement certaines personnes;
- contre les médias traditionnels et les médias sociaux pour y faire de la désinformation et de la propagande, et manipuler les opinions des électeurs¹⁹⁸.

Enfin, le CST croit « qu’il est très probable que les cybermenaces contre les processus démocratiques seront plus nombreuses et plus complexes au cours de l’année à venir, et peut-être à plus long terme » à l’échelle mondiale. Cela s’expliquerait notamment par le fait que « de nombreuses cybercapacités sont accessibles au public, abordables et faciles

194 *Ibid.*, p. 4.

195 *Ibid.*, p. 5.

196 *Ibid.*

197 Un « adversaire » est défini à la p. 12 du rapport comme « tout État, tout groupe ou toute personne qui a utilisé ou qui pourrait utiliser des cybercapacités pour menacer ou influencer le processus démocratique du Canada ».

198 Centre de la sécurité des télécommunications, [*Cybermenaces contre le processus démocratique du Canada*](#), 16 juin 2017, p. 5.

à utiliser » et que « l'expansion rapide des médias sociaux et le déclin des sources d'information faisant autorité rendent la tâche plus facile aux adversaires qui utilisent leurs cybercapacités et d'autres méthodes pour faire des campagnes de désinformation et de propagande dans les médias et influencer les électeurs¹⁹⁹ ».

Des représentants du CST ont comparu le 18 octobre 2018. Dan Rogers, qui est le chef adjoint du SIGINT (pour « signals intelligence » en anglais), a confié au Comité que le CST avait reçu pour consigne de poursuivre son analyse et qu'il s'attend à publier une mise à jour du rapport mentionné précédemment²⁰⁰.

André Boucher, qui est le sous-ministre adjoint aux Opérations du Centre canadien pour la cybersécurité, a précisé que la mise à jour du rapport en question est prévue pour le début de l'année 2019 et il a donné un aperçu de ce qu'on peut en attendre :

Effectivement, il y a une augmentation des menaces. Le principal changement a trait à la vitesse à laquelle les menaces ont augmenté. Nous nous attendions à ce qu'elles augmentent, mais cela s'est fait plus rapidement. Cela s'applique aussi au Canada. Personne n'en sera surpris, compte tenu de ce qui se passe à l'international²⁰¹.

Témoignage de Ben Scott

Ben Scott s'est également penché sur la question de la sécurité. Selon lui,

C'est la pièce la plus simple et la plus importante du casse-tête. L'association de cyberattaques et de campagnes de désinformation que nous avons vu déferler lors des élections dans divers pays est une menace redoutable et il faut la traiter comme telle. Nous devons accroître la cybersécurité de nos institutions démocratiques, non seulement pour l'administration électorale, mais aussi pour les partis politiques et les campagnes. Il faut les traiter comme des infrastructures essentielles, à mon avis. Nous devons aussi mieux coordonner la recherche, la surveillance et l'exposition des campagnes de désinformation associées aux services de sécurité, aux entités de recherche externes et aux entreprises²⁰².

199 *Ibid.*

200 ETHI, *Témoignages*, 1^{re} session, 42^e législature, 18 octobre 2018, 1120 (Dan Rogers, chef adjoint, SIGINT, Centre de la sécurité des télécommunications).

201 ETHI, *Témoignages*, 1^{re} session, 42^e législature, 18 octobre 2018, 1140 (André Boucher, sous-ministre adjoint, Opérations, Centre canadien pour la cybersécurité, Centre de la sécurité des télécommunications).

202 ETHI, *Témoignages*, 1^{re} session, 42^e législature, 25 septembre 2018, 1115 (Ben Scott, directeur, Politiques et défense des intérêts, Omidyar Network).



Témoignage de Maurice Stucke

Faisant un lien entre les questions de concurrence et de sécurité, M. Stucke a fait le constat suivant :

Il y a plusieurs conséquences à une atteinte à la sécurité ou à la violation des politiques relatives aux données des trusts de données. Un trust ou monopole de données est plus enclin à protéger ses données, mais les pirates informatiques sont aussi plus enclins à accéder à ces données, en raison de leur étendue. Les consommateurs peuvent être outrés, mais une entreprise dominante a moins de raisons de craindre que les consommateurs se tournent vers des concurrents²⁰³.

Témoignages de Michael Pal et du directeur général des élections

En ce qui concerne la cybersécurité électorale, Michael Pal a formulé la recommandation suivante :

La cybersécurité coûte cher. Je crois, par exemple, que les banques canadiennes dépensent beaucoup d'argent pour assurer la cybersécurité. Cela s'avérerait difficile pour les partis ou les entités politiques qui sont en pleine campagne électorale. Les partis politiques reçoivent des subventions gouvernementales indirectes par le système de remboursement, par exemple, des dépenses électorales. Il serait peut-être bon d'encourager les dépenses en cybersécurité en leur remboursant une partie de ces coûts²⁰⁴.

M. Perrault, le directeur général des élections, a fait une suggestion qui va dans le même sens :

le Comité voudra peut-être évaluer la nécessité d'accorder éventuellement une subvention spéciale aux partis pour les aider à mettre à niveau et améliorer la sécurité de leurs systèmes informatiques, et examiner des moyens d'établir une subvention équitable. Je me rends compte d'après mes propres investissements à Élections Canada de ce qu'il en coûte. Mais je crois qu'il est dans l'intérêt public, non dans l'intérêt privé des partis politiques, d'avoir les ressources nécessaires pour absorber la hausse du coût de la cybersécurité²⁰⁵.

203 ETHI, *Témoignages*, 1^{re} session, 42^e législature, 4 octobre 2018 1110 (Maurice Stucke, professeur, College of Law, University of Tennessee).

204 ETHI, *Témoignages*, 1^{re} session, 42^e législature, 2 octobre 2018, 1115 (Michael Pal, professeur agrégé, Faculté de droit, section de common law, Université d'Ottawa).

205 ETHI, *Témoignages*, 1^{re} session, 42^e législature, 1^{er} novembre 2018, 1135 (Stéphane Perrault, directeur général des élections, Élections Canada).

Prenant comme exemple ce qui se fait aux États-Unis, M. Pal a également recommandé de rendre publics les protocoles concernant la marche à suivre entre les organismes gouvernementaux en cas de cyberattaque²⁰⁶. Selon lui, « [i]l est crucial que le public puisse se fier aux procédures suivies, parce que s'il ne les connaît pas, il risque de penser qu'un organisme favorise l'un des partis ou qu'un pays étranger s'ingère dans la campagne électorale au nom d'un parti ou d'un ensemble d'entités²⁰⁷. »

CONCLUSIONS ET RECOMMANDATIONS

À la lumière de ce qui précède, le Comité estime que les partis politiques auraient avantage à suivre les recommandations du CST et que le gouvernement aurait avantage à continuer d'étudier la manière dont les cybermenaces affectent nos institutions et notre système électoral.

Pour ces raisons, le Comité recommande :

Recommandation 14 sur les partis politiques et les recommandations du Centre de la sécurité des télécommunications :

Que les partis politiques suivent les recommandations du Centre de la sécurité des télécommunications qui les concernent en matière de cybersécurité électorale.

Recommandation 15 sur le besoin d'étudier les cybermenaces :

Que le gouvernement du Canada continue d'étudier la manière dont les cybermenaces affectent les institutions et le système électoral du Canada.

206 ETHI, *Témoignages*, 1^{re} session, 42^e législature, 2 octobre 2018, 1120 (Michael Pal, professeur agrégé, Faculté de droit, section de common law, Université d'Ottawa).

207 *Ibid.*

CHAPITRE 8 : RECHERCHE, LITTÉRATIE NUMÉRIQUE ET SENSIBILISATION DU PUBLIC

ABSENCE DE RECHERCHE

Plusieurs témoins ont hésité à faire des recommandations trop fermes à l'égard de potentielles mesures législatives ou réglementaires, notant un manque d'information et de recherche sur le phénomène de la désinformation et de la mésinformation. Par exemple, Claire Wardle a noté qu'il n'existe qu'un nombre restreint de recherches empiriques sur ce phénomène, qu'elle nomme troubles de l'information. Elle souligne :

Les défis auxquels nous sommes confrontés sont importants, et il faut faire quelque chose rapidement. Cependant, il s'agit d'une situation extrêmement dangereuse, puisque nous avons si peu de données probantes empiriques sur lesquelles fonder des interventions précises. Afin d'étudier l'impact des troubles de l'information de façon à ce que nous puissions vraiment approfondir nos connaissances, nous devons avoir accès aux données que seules les entreprises technologiques possèdent²⁰⁸.

M^{me} Wardle exhorte donc les gouvernements à faire de la pression sur les plateformes de médias sociaux pour permettre davantage de recherche et un accès aux données de ces plateformes, surtout dans le contexte d'élections. Pour les élections, elle suggère de mettre sur pied une unité de recherche spécifique qui pourrait travailler avec les plateformes de médias sociaux pour exercer des pressions afin de leur dire « nous devons travailler avec vous de façon à comprendre qui dit quoi, et qui fait quoi en conséquence ». M^{me} Wardle estime que nous ne pouvons pas demeurer coincés dans cette boucle infinie où l'on continue de décrier le manque d'accessibilité aux données alors que les plateformes répondent qu'elles ne peuvent pas les fournir en raison de questions de confidentialité²⁰⁹. Elle a expliqué :

Je reviens à mon propos du début et dis que nous avons très peu de recherche à ce sujet. Nous devons réfléchir au préjudice de ces manières de faire, mais lorsque nous commençons à penser au contenu, nous devons avoir accès à ces plateformes pour pouvoir le comprendre.

En outre, en tant que société, nous avons besoin de groupes comprenant des prédicateurs, des éthiciens, des avocats, des militants, des chercheurs et des décideurs, car, en réalité, nous sommes face à la question la plus difficile à laquelle nous ayons été

208 ETHI, *Témoignages*, 1^{re} session, 42^e législature, 16 octobre 2018, 1105 (Claire Wardle).

209 *Ibid.*, 1250.



confrontés [...] nous demandons plutôt à des jeunes hommes de la Silicon Valley de la régler ou — sans arrière-pensée — à des politiciens de divers pays de la régler. C'est que le défi est trop complexe pour un seul groupe.

En fait, il s'agit essentiellement d'un groupe de réflexion. Il s'agit de déchiffrer un code. Quel que soit le problème, nous n'allons pas le régler vite fait. Nous ne devrions pas réglementer rapidement, mais il y a des dommages... Mon inquiétude est que, dans 20 ans, nous repenserons à ces genres de procédures fondées sur des témoignages et dirons que nous nous dirigeons tout droit vers un mur, par automatisme. Je pense que nous n'avons aucune idée du préjudice à long terme²¹⁰.

M. Harris est également d'avis que davantage de recherche est requise sur les effets que les plateformes de médias sociaux ont sur le tissu social. Il ne croit pas que ce soit le rôle du gouvernement de légiférer sur la façon dont les géants de la technologie conçoivent leurs produits, mais qu'ils devraient être tenus responsables des externalités qui sont générées dans la société (p. ex. méfaits de la polarisation). Afin d'être tenus responsables de ces externalités, il est d'avis que « nous avons besoin de plus de recherches, de plus de financement pour ces recherches, afin de montrer quels sont ces méfaits. Nous avons besoin de plus de transparence, car souvent, la seule façon de connaître ces méfaits, c'est d'avoir accès aux données brutes²¹¹ ».

Fenwick McKelvey a dit espérer qu'à l'égard des questions relatives à la publicité en ligne, aux courtiers en données tiers et à l'analyse de données et aux partis politiques que « le Comité songera aux façons d'encourager davantage la recherche dans ces domaines afin que les chercheurs aient un meilleur accès aux données selon des lignes directrices déontologiques claires²¹² ». Ben Scott a quant à lui souligné qu'il est important de « mieux coordonner la recherche, la surveillance et l'exposition des campagnes de désinformation associées aux services de sécurité, aux entités de recherche externes et aux entreprises²¹³ ». Il a suggéré qu'il faut encourager la communauté de recherche à consacrer plus de temps, d'énergie et d'argent à l'étude du problème puisque « [n]ous n'en savons tout simplement pas assez sur la façon dont la désinformation et les marchés fonctionnent pour façonner les points de vue politiques et les résultats électoraux²¹⁴ ».

210 *Ibid.*, 1235.

211 *Ibid.*, 1240 (Tristan Harris).

212 ETHI, *Témoignages*, 1^{re} session, 42^e législature, 25 septembre 2018, 1110 (Fenwick McKelvey).

213 *Ibid.*, 1120 (Ben Scott).

214 *Ibid.*, 1125.

LITTÉRATIE NUMÉRIQUE

En plus du manque de recherche, plusieurs témoins s'entendent sur le fait qu'il faut éduquer les gens davantage à l'égard des menaces qui existent sur les diverses plateformes de médias sociaux et leur apprendre, par exemple, comment vérifier la source de l'information qui est publiée sur leur fil de nouvelles et comment s'assurer que le compte qui transmet l'information est administré par un humain et non par un robot.

Ben Scott a souligné l'importance de se concentrer sur la tâche à long terme de sensibilisation du public, indiquant qu'il faut aider les gens à devenir des consommateurs de médias plus avertis et éclairés²¹⁵. À son avis, la raison pour laquelle les gens sont vulnérables à la désinformation est que ce qui expliquerait pourquoi une plateforme de médias sociaux telle que Facebook a décidé de lui fournir une nouvelle particulière lui échappe. Contrairement aux nouvelles que l'on voit sur CNN ou FoxNews, dans un compte Facebook « 10 000 nouvelles attendent, mais je n'en verrai que 5 %, celles que Facebook décidera de me montrer, d'après ce qu'il pense que je veux voir, non ce que je choisis »²¹⁶. Il est donc important que les gens aient la capacité de distinguer les sources légitimes et illégitimes de contenu et qu'on enseigne des façons rapides et faciles d'évaluer la crédibilité et la qualité de la source²¹⁷.

Elizabeth Dubois a indiqué qu'il faut « éduquer les citoyens en créant par exemple des déclarations de consentement mieux éclairées et en lançant des initiatives de littératie sur les médias et sur la culture numérique²¹⁸ ». Elle estime qu'il serait « crucial d'offrir des programmes de littératie numérique à grande échelle sur le fonctionnement de ces plateformes numériques afin que les citoyens soient en mesure d'exiger la protection que nous leur devons²¹⁹ ».

Bianca Wylie a indiqué qu'il était important de ne pas prendre des décisions trop hâtives dans le débat sur la technologie et la société et que les lois doivent selon elle se faire lentement²²⁰. Elle a offert l'exemple de Sidewalk Labs, un projet de ville intelligente à Toronto. Dans le cadre de ce projet, des consultations publiques ont lieu, mais dans un environnement où selon M^{me} Wylie « personne ne comprend vraiment ce qui se

215 *Ibid.*, 1125 et 1130.

216 *Ibid.*, 1130.

217 *Ibid.*, 1140.

218 ETHI, *Témoignages*, 1^{re} session, 42^e législature, 2 octobre 2018, 1105 (Elizabeth Dubois).

219 *Ibid.*

220 ETHI, *Témoignages*, 1^{re} session, 42^e législature, 4 octobre 2018, 1215 (Bianca Wylie, cofondatrice, Tech Reset Canada).



« passe »²²¹. Elle a invité le Comité à « réfléchir à tout ce qu'il nous faut faire en matière d'éducation avant même que la collectivité puisse prendre des décisions éclairées » en matière de technologie²²². Selon elle, il est important de sensibiliser la population à ce qui se passe actuellement en ce qui concerne les données et la protection de la vie privée²²³.

Ryan Black a également souligné l'importance de l'éducation en indiquant que son collègue et lui estiment « que l'intervention des gouvernements doit consacrer suffisamment de ressources à l'éducation, à la compréhension du monde numérique et des nouvelles et à l'esprit critique²²⁴ ». Il a rajouté qu'à son avis l'éducation du public, par exemple à l'aide d'une campagne de sensibilisation, pourrait être plus efficace qu'un outil législatif visant à réglementer les plateformes de médias sociaux²²⁵.

SENSIBILISATION DU PUBLIC

M. Scott indique que la sensibilisation du public doit passer non seulement par la littératie numérique, mais par des investissements substantiels dans de meilleurs médias indépendants. Selon lui « [n]ous ne pouvons pas nous attendre à ce que les gens s'éloignent des absurdités qui se trouvent sur Internet s'il n'y a pas de grandes quantités de renseignements et d'articles journalistiques de qualité à leur disposition²²⁶ ».

M. Owen est d'avis qu'il « est manifestement essentiel, dans une démocratie, d'avoir des renseignements fiables qui sont connus d'un grand nombre de citoyens ». Par conséquent il estime qu'il faut examiner la façon par laquelle nous favorisons le renforcement de la fiabilité des renseignements dans l'écosystème d'information numérique et que cela passe par le journalisme fiable²²⁷.

M. McKelvey a quant à lui souligné qu'une partie de l'intégrité de notre démocratie repose sur le financement de la radiodiffusion publique.

221 *Ibid.*, 1105.

222 *Ibid.*

223 *Ibid.*, 1215.

224 ETHI, *Témoignages*, 1^{re} session, 42^e législature, 16 octobre 2018, 1210 (Ryan Black, (associé, coprésident du groupe des technologies de l'information, McMillan LLP).

225 *Ibid.*, 1210.

226 ETHI, *Témoignages*, 1^{re} session, 42^e législature, 25 septembre 2018, 1125 et 1130 (Ben Scott).

227 *Ibid.*, 1220 (Taylor Owen).

Au Canada, nous avons dit avoir une politique culturelle proactive et agir comme pourvoyeur d'information pour le bien de la population. Quand on parle de confiance à l'égard des médias, on peut dire que la radiodiffusion publique a été vraiment efficace pour élever la barre, pour freiner les campagnes d'information trompeuse ou de désinformation, et pour diffuser de l'information de qualité. Il m'apparaît très clairement que la radiodiffusion publique sert l'intérêt public, et c'est encore plus vrai aujourd'hui. C'est unique, et cela doit continuer de faire partie de la solution optimale que le Canada apportera aux problèmes soulevés²²⁸.

Enfin, M^{me} Wardle a aussi noté l'importance de soutenir le journalisme de qualité, offrant comme exemple un projet mené durant les récentes élections brésiliennes où vingt-quatre grandes salles de rédaction ont travaillé de concert afin de combattre la désinformation²²⁹.

Le Comité reconnaît le besoin de plus de recherche et d'efforts en matière de littératie numérique et de sensibilisation du public et recommande par conséquent :

Recommandation 16 sur la recherche en matière de désinformation et de mésinformation en ligne :

Que le gouvernement du Canada investisse des ressources dans la recherche sur les impacts de la désinformation et de la mésinformation en ligne.

Recommandation 17 sur l'éducation et la littératie numérique :

Que le gouvernement du Canada augmente ses investissements en matière d'initiatives de littératie numérique, y compris à l'égard d'initiatives visant à informer les Canadiens des risques liés à la propagation de désinformation et de mésinformation en ligne.

Le Comité tient aussi à souligner que les plateformes de médias sociaux, en particulier Facebook, qui n'a pas été le meilleur citoyen corporatif au cours des dernières années, devraient aussi fournir du temps et des ressources financières aux initiatives de littératie numérique et de sensibilisation du public. Leur influence est immense et leur responsabilité sociale est importante.

Comme le démontre la preuve entendue au cours de cette étude, les problèmes structurels inhérents des plateformes de médias sociaux, qui sont tributaires de l'économie de l'attention, font en sorte que les utilisateurs consomment sans cesse l'information et deviennent essentiellement dépendants des services qui leur sont

228 *Ibid.*, 1205 et 1245 (Fenwick McKelvey).

229 ETHI, *Témoignages*, 1^{re} session, 42^e législature, 16 octobre 2018, 1240 (Claire Wardle).



offerts. Qui plus est, les puissants algorithmes utilisés sur ces plateformes font la promotion de contenu sur la base de principes n'étant pas toujours favorables à la démocratie, mais plutôt dans le but de maximiser les revenus publicitaires ou de susciter l'intérêt des utilisateurs en manipulant le contenu qu'ils voient.

Cette combinaison de facteurs fait en sorte que la façon d'opérer des plateformes de médias sociaux semble contribuer grandement à la propagation rapide de désinformation et de mésinformation en ligne. Cette réalité soulève, de l'avis du Comité, des questions éthiques importantes.

Ces questions éthiques devront être résolues si l'on veut qu'à l'avenir les géants de la technologie réduisent leurs externalités négatives et empêchent les acteurs malveillants d'utiliser leurs outils disponibles gratuitement en ligne afin de rapidement propager du contenu faux, incitant à la haine, divisif, polarisant ou toute autre forme de désinformation ou de mésinformation. Afin que le gouvernement du Canada soit un leader en la matière, le Comité recommande donc :

Recommandation 18 sur le caractère addictif de certains produits numériques :

Que le gouvernement du Canada étudie les effets cognitifs à long terme des produits numériques favorisant la dépendance qui sont offerts par les plateformes sociales, et qu'il détermine si une réponse est requise.

Les 18 recommandations formulées par le Comité ci-dessus apportent des nuances ou plus de détails à certaines des recommandations préliminaires contenues dans son rapport provisoire, et incluent de nouvelles recommandations sur des concepts nouveaux étudiés à l'automne. Le Comité souhaite donc réitérer ses recommandations préliminaires :

Recommandation 19 sur la transparence :

Que le gouvernement du Canada établisse des exigences sur la transparence relativement à la collecte et à l'utilisation des données que font les organisations et les acteurs politiques, particulièrement au moyen des médias sociaux et d'autres plateformes en ligne afin de cibler la publicité politique ou autre à l'aide de techniques comme le profilage psycho-graphique. Ces exigences pourraient inclure, sans s'y limiter :

- **L'identification de la personne qui a payé pour la publicité, y compris la vérification de l'authenticité de la personne qui diffuse la publicité;**

- L'identification du public cible et la raison pour laquelle le public cible a reçu la publicité; et
- L'enregistrement obligatoire concernant la publicité politique à l'extérieur du Canada.

Recommandation 20 sur la mise en œuvre au Canada de mesures semblables à celles du *Règlement général sur la protection des données* :

Que le gouvernement du Canada mette immédiatement en œuvre des mesures pour veiller à ce que des protections semblables à celles du *Règlement général sur la protection des données* soient mises en place au Canada, y compris les recommandations contenues dans le rapport sur la *Loi sur la protection des renseignements personnels et les documents électroniques* présenté en février 2018.

Recommandation 21 sur la souveraineté des données :

Que le gouvernement du Canada établisse des règles et des lignes directrices sur la propriété des données et la souveraineté des données afin de mettre un terme à la collecte et à l'utilisation non autorisées des renseignements personnels des citoyens. Ces règles et lignes directrices devraient tenir compte des défis que représente l'infonuagique.

Recommandation 22 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.

Recommandation 23 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.



Recommandation 24 sur des pouvoirs d'exécution additionnels 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 d'émettre des avis urgents à une organisation relativement à la production de documents pertinents dans une durée plus courte et le pouvoir de saisir des documents dans le cadre d'une enquête, sans préavis.

Recommandation 25 sur le partage d'information entre le commissaire à la protection de la vie privée et d'autres organismes de régulation :

Que la *Loi sur la protection des renseignements personnels et les documents électroniques* soit modifiée afin d'autoriser le commissaire à la protection de la vie privée à partager certaines informations pertinentes dans le cadre d'enquêtes avec le Bureau de la concurrence, d'autres organismes de régulation canadiens et des organismes de régulation à l'échelle internationale, lorsque cela est approprié.

Recommandation 26 sur l'application des lois relatives à la protection de la vie privée aux activités politiques :

Que le gouvernement du Canada prenne certaines mesures afin d'assurer l'application de la législation en matière de protection de la vie privée aux activités politiques, soit par la modification des lois existantes ou par l'adoption d'une nouvelle loi.

CONCLUSION

Le commissaire à la protection de la vie privée n'a pas mâché ses mots en décrivant l'état de la situation actuelle : une crise dans le domaine de la collecte et du traitement des renseignements personnels en ligne. Le Comité ne prend pas ces remarques à la légère et estime que le fait qu'il ait tiré la sonnette d'alarme rend ses recommandations d'autant plus importantes.

En cette fin d'étude, le Comité demeure persuadé que des changements au paysage législatif et réglementaire canadien doivent être apportés si l'on veut radier la menace que les campagnes de désinformation et de mésinformation font planer sur le processus démocratique de notre pays.

Il est impératif que le gouvernement du Canada soit un chef de file dans la mise en place de solutions législatives durables qui permettront de protéger les renseignements personnels des Canadiens, sans être un boulet pour l'innovation. Il doit aussi investir le temps et les ressources nécessaires afin de mieux informer les citoyens canadiens des dangers qui existent à l'ère de la désinformation et des monopoles de données. Bref, aucun effort ne doit être épargné afin de permettre aux Canadiens de participer à l'économie numérique et au processus démocratique sans crainte.

Enfin, le Comité soutient que si les événements de la dernière année ont révélé une chose, c'est que les plateformes de médias sociaux devraient faire un réel exercice d'introspection, car elles ont un choix important à faire. Veulent-elles continuer d'exercer leurs activités dans un modèle d'affaires destiné à créer une dépendance à leurs services tout en faisant abstraction des effets nocifs qu'elles peuvent créer dans notre tissu social et de l'impact à long terme sur les humains? Ou veulent-elles au contraire réaligner la technologie d'une façon plus éthique et compatible avec les capacités de l'esprit humain? Le Comité espère sincèrement qu'elles choisiront la deuxième option.

ANNEXE A

LISTE DES TÉMOINS

Le tableau ci-dessous présente les témoins qui ont comparu devant le Comité lors des réunions se rapportant au présent rapport. Les transcriptions de toutes les séances publiques reliées à ce rapport sont affichées sur la [page Web du Comité sur cette étude](#).

| Organismes et individus | Date | Réunion |
|---|------------|---------|
| À titre personnel | 2018/04/17 | 99 |
| Chris Vickery, directeur de la recherche sur les risques cybernétiques UpGuard | | |
| Commissariat à la protection de la vie privée du Canada | 2018/04/17 | 99 |
| Barbara Bucknell, directrice Politiques, affaires parlementaire et recherche Daniel Therrien, commissaire à la protection de la vie privée du Canada | | |
| Facebook Inc. | 2018/04/19 | 100 |
| Kevin Chan, directeur mondial et chef de la politique publique Facebook Canada Robert Sherman, directeur adjoint de la protection des renseignements personnels | | |
| AggregatelQ | 2018/04/24 | 101 |
| Zackary Massingham, directeur général Jeff Silvester, chef des opérations | | |
| À titre personnel | 2018/04/26 | 102 |
| Colin J. Bennett, professeur Département de science politique, University of Victoria Thierry Giasson, professeur titulaire Département de science politique, Université Laval | | |
| Mozilla Corporation | 2018/04/26 | 102 |
| Marshall Erwin, directeur Fiducie et Sécurité | | |

| Organismes et individus | Date | Réunion |
|--|-------------|----------------|
| Chambre des communes du Royaume-Uni, Comité spécial sur le numérique, la culture, les médias et le sport Damian Collins, président, député | 2018/05/03 | 104 |
| Bureau de la commissaire à l'information du Royaume-Uni Elizabeth Denham, commissaire à l'information | 2018/05/10 | 106 |
| Bureau du Commissaire à l'information et à la protection de la vie privée de la Colombie-Britannique Michael McEvoy, commissaire | 2018/05/10 | 106 |
| Conseil des innovateurs canadiens Jim Balsillie, président | 2018/05/10 | 106 |
| Google Canada Colin McKay, chef, politiques publiques et relations gouvernementales | 2018/05/10 | 106 |
| Chambre des communes André Gagnon, sous-greffier, procédure Chambre des communes Wendy Gordon, directrice, affaires législatives Bureau du légiste et conseiller parlementaire Stéphane am Rhyn, avocat Bureau du légiste et conseiller parlementaire | 2018/05/24 | 108 |
| À titre personnel Christopher Wylie | 2018/05/29 | 109 |
| Commissariat à la protection de la vie privée du Canada Barbara Bucknell, directrice Politiques, affaires parlementaire et recherche Brent Homan, directeur exécutif Direction de la conformité de la Loi sur la protection des renseignements personnels et les documents électroniques Sarah Speevak, conseillère juridique Daniel Therrien, commissaire à la protection de la vie privée du Canada | 2018/05/31 | 110 |

| Organismes et individus | Date | Réunion |
|---|-------------|----------------|
| À titre personnel Chris Vickery, directeur de la recherche sur les risques cybernétiques UpGuard | 2018/06/07 | 112 |
| AggregatelQ Jeff Silvester, chef des opérations | 2018/06/12 | 113 |
| À titre personnel Fenwick McKelvey, professeur agrégé Études en communications, Université Concordia Taylor Owen, professeur agrégé Médias numériques et affaires mondiales, University of British Columbia | 2018/09/25 | 116 |
| Omidyar Network Ben Scott, directeur Politiques et défense des intérêts | 2018/09/25 | 116 |
| AggregatelQ Zackary Massingham, directeur général | 2018/09/27 | 117 |
| À titre personnel Samantha Bradshaw, chercheuse Elizabeth Dubois, professeure adjointe Département de communication, Université d'Ottawa Michael Pal, professeur agrégé Faculté de droit, section de common law, Université d'Ottawa | 2018/10/02 | 118 |
| À titre personnel Maurice Stucke, professeur College of Law, University of Tennessee | 2018/10/04 | 119 |
| Tech Reset Canada Bianca Wylie, cofondatrice | 2018/10/04 | 119 |

| Organismes et individus | Date | Réunion |
|--|-------------|----------------|
| À titre personnel Ryan Black, associé coprésident du groupe des technologies de l'information, McMillan LLP Vivian Krause, chercheuse et rédactrice Pablo Jorge Tseng, avocat McMillan LLP Claire Wardle Harvard University | 2018/10/16 | 120 |
| Centre for Humane Technology Tristan Harris, cofondateur et directeur exécutif | 2018/10/16 | 120 |
| Banque du Canada Eric Santor, directeur général Analyses de l'économie canadienne | 2018/10/18 | 121 |
| Bureau de la concurrence Anthony Durocher, sous-commissaire Direction des pratiques monopolistiques Alexa Gendron-O'Donnell, sous-commissaire déléguée, direction de l'analyse économique Direction générale de la promotion de la concurrence | 2018/10/18 | 121 |
| Centre de la sécurité des télécommunications André Boucher, sous-ministre adjoint Opérations, Centre canadien pour la cybersécurité Dan Rogers, chef adjoint SIGINT | 2018/10/18 | 121 |
| Google Canada Colin McKay, chef, politiques publiques et relations gouvernementales | 2018/10/23 | 122 |
| Nouveau Parti démocratique Jesse Calvert, directeur des opérations | 2018/10/30 | 123 |
| Parti conservateur du Canada Trevor Bailey, agent de la protection de la vie privée et directeur des adhésions | 2018/10/30 | 123 |

| Organismes et individus | Date | Réunion |
|---|-------------|----------------|
| Parti libéral du Canada Michael Fenrick, conseiller juridique et constitutionnel Conseil national d'administration | 2018/10/30 | 123 |
| Commissariat à la protection de la vie privée du Canada Julia Barss, avocate générale et directrice des services juridiques Direction des services juridiques Brent Homan, sous-commissaire Secteur de la conformité Gregory Smolynec, sous-commissaire Secteur des politiques et de la promotion Daniel Therrien, commissaire à la protection de la vie privée du Canada | 2018/11/01 | 124 |
| Conseil de la radiodiffusion et des télécommunications canadiennes Neil Barratt, directeur Mise en application du commerce électronique Rachelle Frenette, conseillère juridique Scott Hutton, directeur exécutif Radiodiffusion | 2018/11/01 | 124 |
| Élections Canada Anne Lawson, sous-directrice générale des élections Affaires réglementaires Stéphane Perrault, directeur général des élections | 2018/11/01 | 124 |

ANNEXE B

LISTE DES MÉMOIRES

Ce qui suit est une liste alphabétique des organisations et des personnes qui ont présenté au Comité des mémoires reliés au présent rapport. Pour obtenir de plus amples renseignements, veuillez consulter la [page Web du Comité sur cette étude](#).

Eatz, Sydney

Oath inc.

DEMANDE DE RÉPONSE DU GOUVERNEMENT

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

Un exemplaire des *procès-verbaux* pertinents (réunions nos 99 à 102, 104, 106, 108 à 114, 116 à 124 et 127 à 129) est déposé.

Respectueusement soumis,

Le président,
Bob Zimmer

