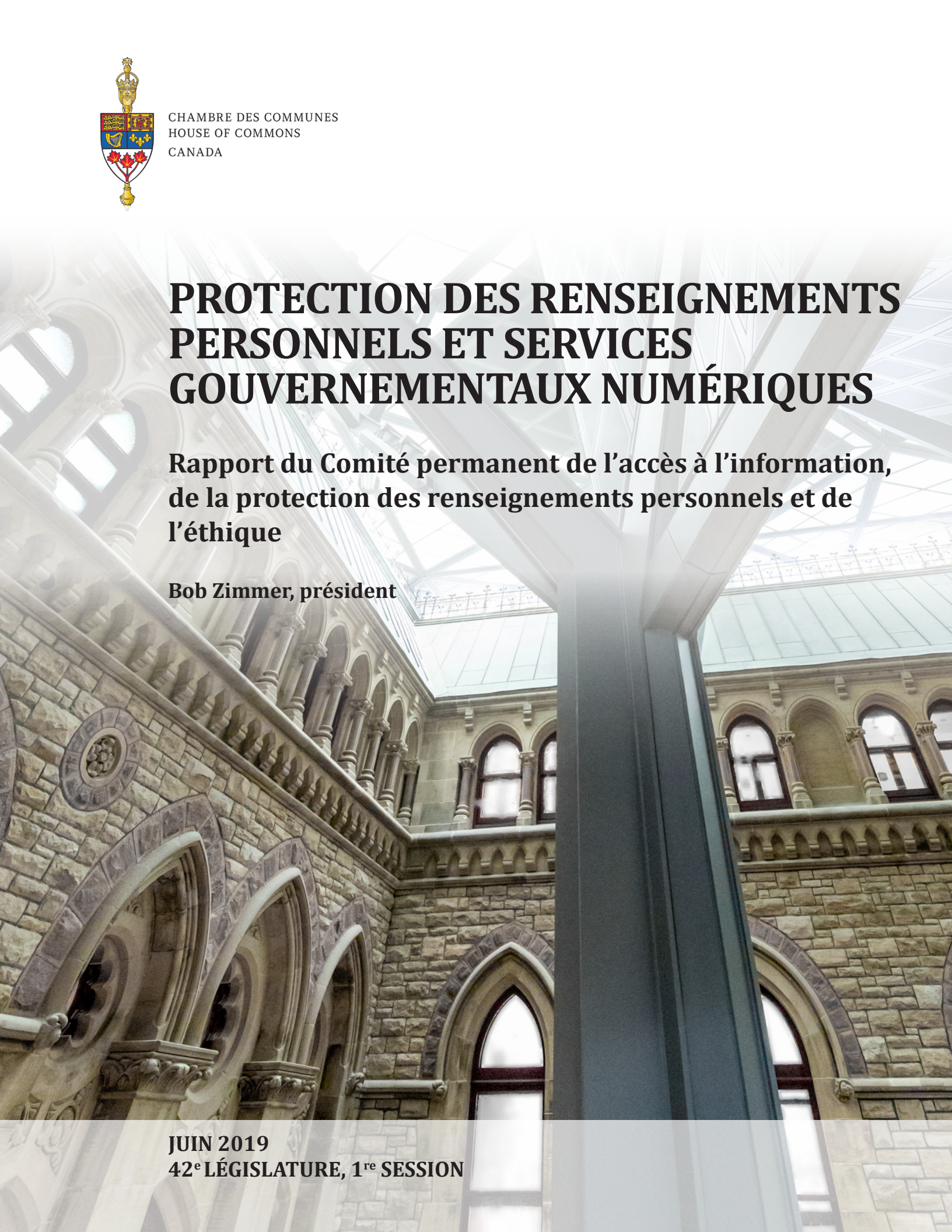
CHAMBRE DES COMMUNES
HOUSE OF COMMONS
CANADA

PROTECTION DES RENSEIGNEMENTS PERSONNELS ET SERVICES GOUVERNEMENTAUX NUMÉRIQUES

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

Bob Zimmer, président



JUIN 2019
42e LÉGISLATURE, 1re SESSION

PROTECTION DES RENSEIGNEMENTS PERSONNELS ET SERVICES GOUVERNEMENTAUX NUMÉRIQUES

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

Le président
Bob Zimmer

JUIN 2019

42e LÉGISLATURE, 1re 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

Hon. Peter Kent

Michel Picard

Raj Saini

Anita Vandenbeld

AUTRES DÉPUTÉS QUI ONT PARTICIPÉ

Ziad Aboultaif

René Arseneault

Nathan Cullen

Fayçal El-Khoury

Andy Fillmore

David de Burgh Graham

Cheryl Hardcastle

Gord Johns

Michael Levitt

Brian Masse

Irene Mathyssen

Robert J. Morrissey

L’hon. Joyce Murray
Eva Nassif
Anne Minh-Thu Quach
Churence Rogers
Francis Scarpaleggia
Gagan Sikand
Adam Vaughan

GREFFIERS DU COMITÉ

Michael MacPherson
Jean-Denis Kusion

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-NEUVIÈME RAPPORT

Conformément à l'article 108(3)*h*)(vii) du Règlement, le Comité a étudié la protection des données personnelles dans les services gouvernementaux numériques et a convenu de faire rapport de ce qui suit :

TABLE DES MATIÈRES

LISTE DES RECOMMANDATIONS

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

Recommandation 1 sur la modernisation des lois relatives à la protection des renseignements personnels du Canada :

Que la *Loi sur la protection des renseignements personnels* et la *Loi sur la protection des renseignements personnels et les documents électroniques* soient modernisées en adoptant les recommandations du Comité relatives à ces lois dans les rapports suivants :

- **Rapport 4 — Protéger la vie privée des Canadiens : examen de la Loi sur la protection des renseignements personnels (décembre 2016)**
- **Rapport 12 — Vers la protection de la vie privée dès la conception : Examen de la Loi sur la protection des renseignements personnels et les documents électroniques (février 2018)**
- **Rapport 16 — Aborder les vulnérabilités de la vie privée numérique et les menaces potentielles au processus électoral démocratique canadien (juin 2018)**
- **Rapport 17 — Démocratie menacée : risques et solutions à l'ère de la désinformation et du monopole des données (décembre 2018) 21**

Recommandation 2 sur la minimisation des données :

Que le gouvernement du Canada s'engage à respecter la minimisation des données, à dépersonnaliser tous les renseignements personnels à la source lorsqu'ils sont recueillis à des fins de recherche ou à des fins semblables et à clarifier les règles de consentement concernant l'échange de renseignements personnels entre ministères et agences gouvernementales. 22

PROTECTION DES RENSEIGNEMENTS PERSONNELS ET SERVICES GOUVERNEMENTAUX NUMÉRIQUES

INTRODUCTION

Le 6 février 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 adopté une motion visant à ce que le Comité entreprenne une étude sur les services gouvernementaux numériques afin de comprendre comment le gouvernement peut améliorer les services offerts aux Canadiens tout en protégeant leur vie privée et leur sécurité[1].

Le Comité a tenu 12 réunions avec témoins sur le sujet, entre le 22 mars 2018 et le 9 avril 2019, au cours desquelles il a entendu un total de 33 témoins. Il a également reçu quatre mémoires.

Le présent rapport résume les témoignages entendus par le Comité et formule huit recommandations.

LE MODÈLE ESTONIEN

L'étude menée par le Comité a été inspirée par le modèle de gouvernement numérique en Estonie, qui est l'un des pays les plus avancés en matière de services gouvernementaux numériques. Afin de mieux comprendre ce modèle et comment il a été possible de créer une société numérique dans ce pays, le Comité a reçu, comme premiers témoins de cette étude, des représentants de l'Académie de la cybergouvernance de l'Estonie.

A. Représentants de l'Estonie

Au sujet des principes fondateurs du modèle de cybergouvernance de l'Estonie, Liia Hänni, experte de haut niveau en cyberdémocratie à l'Académie de la cybergouvernance de l'Estonie, a souligné qu'il repose sur la conviction qu'une structure

1 Chambre des communes, Comité permanent de l'accès à l'information, de la protection des renseignements et de l'éthique (ETHI), *Procès-verbal*, 1re session, 42e législature, 6 février 2018.

et un modèle de gouvernance numérique devaient être une plateforme pour toute la société[2]. Selon elle, le modèle estonien compte trois composantes importantes :

- le gouvernement estonien donne une forte identité numérique aux Estoniens;
- les données et les ressources numériques sont nombreuses (des centaines de bases de données pouvant accueillir des données numériques existent);
- l'interopérabilité entre les nombreux ensembles de données est assurée par la plateforme X-Road qui permet de connecter tous les ensembles de données dans un seul système uniforme[3].

M[me] Hänni a souligné que l'expérience estonienne a démontré que l'on pouvait mieux protéger les renseignements personnels dans un environnement numérique que dans un environnement papier. En Estonie, les citoyens peuvent retracer les échanges d'information numériques qui ont lieu, qui a consulté leur dossier et pourquoi. Il est souvent impossible de savoir qui a consulté des documents papier et pourquoi[4].

Elle a aussi mentionné que les signatures électroniques sont chose courante dans son pays. Les Estoniens n'ont plus besoin de signer des documents papier, et la signature électronique permet au pays de faire une énorme « économie de ressources, de temps et d'argent[5] ».

En ce qui concerne l'aspect cybersécurité du modèle estonien, Raul Rikk, directeur du Programme de cybersécurité nationale de l'Académie de la cybergouvernance de l'Estonie, a expliqué que tous les Estoniens possèdent une carte d'identité avec une puce dotée d'un cryptoprocesseur. Quand ils s'en servent, ils utilisent en fait un système de cryptage[6]. La carte d'identité est livrée par le gouvernement et grâce au processus

2 ETHI, *Témoignages*, 1re session, 42e législature, 22 mars 2018; Académie de la cybergouvernance de l'Estonie, *About Us* [DISPONIBLE EN ANGLAIS SEULEMENT].

3 ETHI (2018), 0905 (Liia Hänni, experte en cyberdémocratie, Académie de la cybergouvernance de l'Estonie).

4 *Ibid*., 0940.

5 *Ibid*., 1010.

6 *Ibid*., 0915 (Raul Rikk, directeur, Programme de cybersécurité nationale, Académie de la cybergouvernance de l'Estonie).

gouvernemental d'identification des personnes et de délivrance des cartes d'identité, l'Estonie s'assure que personne ne peut voler l'identité d'une autre personne[7].

M. Rikk a expliqué que la collecte de données effectuée par diverses entités estoniennes repose sur le principe de la « demande unique » :

> Nous n'avons pas centralisé les bases de données, mais la logique qui sous-tend le principe du non-chevauchement des bases de données, c'est que nous ne recueillons pas les mêmes données dans différentes bases de données. Par exemple, s'il y a un registre de la population contenant les renseignements de base au sujet des citoyens et des résidents, alors, lorsque les services de police créent leur propre base de données, nous ne leur permettons pas de recueillir les mêmes renseignements de base. Ils doivent prendre les renseignements les plus récents figurant dans le registre de la population. L'idée, c'est que les différentes institutions étatiques ont un pouvoir lié à certaines données. Si on leur permet de recueillir et de conserver ces données dans leur base de données, alors personne d'autre ne peut recueillir et conserver les mêmes données. De cette façon, nous maintenons de l'ordre dans les données à l'échelon national[8].

M. Rikk a précisé qu'aucun organisme en Estonie n'est en mesure d'accéder à toute l'information échangée d'un seul coup. Seules les personnes autorisées consultent les ensembles de données. Les droits d'accès diffèrent si on est citoyen, fonctionnaire ou policier[9]. Il existe aussi un registre de tous les accès aux données des citoyens que ceux-ci peuvent consulter sur le portail de l'État afin de savoir qui a vu quelle information à quel moment. Seuls les citoyens concernés peuvent voir l'ensemble des données recueillies sur eux[10].

M. Rikk a aussi indiqué que la nature décentralisée des renseignements permet de gérer les vulnérabilités possibles d'un système de gestion de l'information. L'Estonie ne possède pas une seule immense base de données qui contient tous les renseignements sur ses citoyens. Par conséquent, si une personne pénètre dans certains systèmes et les endommage, les dégâts seront circonscrits à un seul système distinct contenant de l'information et non pas à l'entièreté du système[11]. M. Rikk a décrit l'échange de renseignements entre les bases de données en Estonie :

---

7 *Ibid*., 0930.

8 *Ibid*., 0915.

9 *Ibid*., 0925.

10 *Ibid*., 0930.

11 *Ibid*., 0950.

> Certaines sont du secteur public, et d'autres, du secteur privé. Nous assurons la connectivité entre les bases de données grâce à un environnement d'échange de données sécurisées. C'est ce que nous appelons X-Road. C'est un environnement contrôlé par l'État. Toute personne voulant se connecter à cet environnement d'échange de données doit, dans un premier temps, appliquer certains règlements en matière de sécurité, des lignes directrices en la matière, pour respecter les règles et ainsi de suite. L'entité doit ensuite présenter une demande pour se joindre à l'environnement d'échange de données sécurisées. Cela signifie que nous gardons un œil sur l'échange de données. Nous le contrôlons. Nous ne consultons pas les données elles-mêmes, mais nous contrôlons de quelle façon l'échange de données se produit. Tout est chiffré, comme je l'ai mentionné, consigné et horodaté. La façon dont nous obtenons de l'information des bases de données, ce n'est pas en interrogeant directement la base de données. Nous obtenons plutôt l'information par l'intermédiaire des services électroniques […]. Il y a la police numérique, l'école numérique, le soutien technique numérique. C'est un peu comme un type de présentation. Le service électronique tire des données prédéfinies des différentes bases de données puis les présente[12].

M. Rikk a insisté sur l'importance de préserver l'intégrité et la confidentialité des renseignements tout en assurant l'accès aux données, en les protégeant et en empêchant leur modification par d'autres personnes que celle à laquelle les données se rapportent[13].

Enfin, en ce qui concerne l'accès du secteur privé aux renseignements des citoyens, M. Rikk a indiqué :

> Chaque fois qu'un intervenant du secteur privé veut utiliser des données personnelles ou veut obtenir une connexion à l'environnement X-Road, il doit prouver son besoin à l'inspecteur responsable de la protection des données. Il doit justifier pourquoi il a besoin de l'accès. L'inspectorat lui permet d'utiliser des données personnelles […] Le secteur privé génère certains renseignements, et il peut les fournir au gouvernement de façon sécurisée par l'intermédiaire de X-Road[14].

B. Commentaires d'autres témoins à l'égard du modèle estonien

Ann Cavoukian, ancienne commissaire à la protection de la vie privée de l'Ontario et experte en résidence du Privacy by Design Centre of Excellence de l'Université Ryerson, a souligné que le modèle estonien était un excellent modèle de décentralisation et qu'un modèle décentralisé comporte plusieurs grappes d'information, chacune des bases de

12 *Ibid*.

13 *Ibid*., 0920.

14 *Ibid*., 1020.

données contenant des renseignements auxquels on peut accéder pour un but précis[15]. À son avis « plus vous avez des grappes d'information décentralisées, plus il est probable que les données restent intactes et qu'elles soient conservées aux fins prévues, au lieu d'être utilisées systématiquement pour une foule de raisons qui n'avaient jamais été envisagées[16] ».

Le commissaire à la protection de la vie privée du Canada, Daniel Therrien, a constaté ce qui suit :

> On parle souvent du modèle estonien en raison de son architecture technologique, mais j'ai remarqué que les représentants ont plutôt mis l'accent sur l'importance des facteurs liés à l'attitude, y compris le besoin de surmonter les cloisonnements administratifs de l'État afin de réutiliser des renseignements personnels à des fins autres que celles pour lesquelles ils ont été recueillis.
>
> Cela pourrait être considéré comme une validation de l'opinion selon laquelle notre *Loi sur la protection des renseignements personnels* doit être réexaminée et les « obstacles juridiques » doivent être éliminés. J'aimerais toutefois souligner qu'en Estonie, l'élimination des cloisonnements n'a pas entraîné une gestion horizontale tout azimut des données personnelles à l'échelle du gouvernement. Dans le modèle estonien, la réutilisation — ou la communication des renseignements personnels — semble plutôt fondée sur des lois généralement conformes aux principes de vie privée reconnus à l'échelle mondiale et au *Règlement général sur la protection des données* [RGPD de l'Union européenne].
>
> […]
>
> En ce qui concerne les aspects technologiques du modèle estonien, nous comprenons qu'il n'existe pas de base de données centralisée. L'accès est plutôt accordé grâce à la capacité de relier des serveurs individuels au moyen de voies d'accès cryptées avec accès ou réutilisation autorisés à des fins légitimes déterminées. Ce système qui limite l'accès à des fins précises par les organismes gouvernementaux est susceptible de réduire le profilage.
>
> Nous comprenons également que des mesures de protection de la vie privée et de sécurité sont prises au moyen du cryptage et de l'utilisation de la chaîne de blocs. Cela est conforme à l'une de nos recommandations de 2016 concernant la refonte de la *Loi sur la protection des renseignements personnels*, à savoir de créer une obligation

15 ETHI, *Témoignages*, 1re session, 42e législature, 29 janvier 2019, 1555 (Ann Cavoukian, Privacy by Design Centre of Excellence, Ryerson University).

16 *Ibid*.

juridique pour les institutions gouvernementales de protéger les renseignements personnels[17].

M. Therrien a tout de même soulevé quelques questions à l'égard du modèle estonien. D'abord, constatant qu'aucun système n'est entièrement sécuritaire, il croit qu'il serait important de connaître les mesures d'atténuation qui existent en Estonie dans le cas d'une atteinte à la sécurité. Il a aussi questionné comment la valeur d'un modèle comme celui de l'Estonie, qui réside dans l'analyse des données détenues par l'ensemble du gouvernement, pourrait être reproduite au Canada, étant donné la décentralisation des ensembles de données et du régime législatif qui limite la réutilisation des données au Canada[18].

Chris Vickery, expert en cybersécurité, a soulevé des doutes à l'égard des affirmations des représentants de l'Estonie qui témoignent n'avoir jamais connu d'atteinte à la protection des données ou de problème les concernant. Il s'est dit convaincu que le système estonien n'est pas impénétrable[19].

David Eaves, conférencier en politiques publiques du projet digital HKS à la Harvard Kennedy School, a souligné trois éléments du modèle estonien qu'il considère importants :

1. une base de données existe pour chaque renseignement recueilli d'un citoyen estonien (p. ex. une pour le lieu de résidence, une pour le permis de conduire, etc.);

2. les renseignements sont liés entre eux par un identifiant unique afin de pouvoir facilement en extraire des éléments d'information disparates au sujet d'un citoyen, de les regrouper pour obtenir un portrait très clair de la personne et transmettre ces renseignements aux différents organismes gouvernementaux à mesure qu'ils tentent d'offrir des services;

3. ces bases de données sont accessibles à tous les fonctionnaires de l'ensemble des services gouvernementaux[20].

---

17 ETHI, *Témoignages*, 1re session, 42e législature, 31 janvier 2019, 1540 (Daniel Therrien, Commissaire à la protection de la vie privée du Canada).

18 *Ibid.*

19 ETHI, *Témoignages*, 1re session, 42e législature, 5 février 2019, 1615 et 1655 (Chris Vickery).

20 ETHI, *Témoignages*, 1re session, 42e législature, 7 février 2019, 1550 (David Eaves, conférencier en politiques publiques, Digital HKS, Harvard Kennedy School).

M. Eaves a aussi soumis un mémoire au Comité consistant en un article qu'il a coécrit intitulé « Lessons from Estonia on digital government[21] ». Dans l'article, les auteurs expliquent que contrairement à plusieurs pays où les services gouvernementaux numériques se développent en silos, certains pays, dont l'Estonie, utilisent un système standardisé qui permet aux divers ministères et agences de partager l'information de connexion et les bases de données qui supportent les services offerts en ligne. De tels systèmes peuvent communiquer entre eux, ce qui permet le développement rapide et moins dispendieux de nouveaux services gouvernementaux numériques. Dans une approche en silos, puisque les ministères numérisent leurs services et fonctionnent de façon indépendante des autres, ils dupliquent les efforts afin de recueillir tous les renseignements personnels nécessaires, ce qui est inefficace et coûteux. La duplication se fait même parfois dans le même ministère.

Dans un « gouvernement de plateformes », des normes sont définies afin qu'il y ait un noyau d'outils et de bases de données, les plateformes, qui puissent être réutilisés par le secteur public et privé afin de réduire les coûts liés à ces services et de les simplifier. Les plateformes gouvernementales sont vues comme une infrastructure publique de base et la source d'un avantage compétitif. Les auteurs reconnaissent cependant l'existence de certains défis liés au virage vers le gouvernement de plateformes, notamment :

- l'entité qui contrôlera les serveurs du gouvernement contrôlera le gouvernement. Le gouvernement pourrait donc avoir intérêt à refuser l'accès à certaines parties des systèmes (p. ex. aux entreprises privées qui participent à l'infrastructure) et s'assurer de contrôler la façon dont ils ont été élaborés;

- les fournisseurs de logiciels privés détermineront l'architecture des services et pourraient les concevoir de manière à gêner la concurrence;

- il pourrait être difficile de convaincre les fonctionnaires et le public de faire confiance aux plateformes communes dans un système qui s'articule autour de ministères cloisonnés.

Selon Alex Benay, le dirigeant principal de l'information du gouvernement du Canada, bien que le Canada soit différent de l'Estonie sur le plan culturel et juridique, son organisation a beaucoup appris de ce pays y compris comment échanger des données de

21 David Eaves and Ben McGuire, « Lessons from Estonia on digital government », Options politiques, 7 février 2019. L'article contient entre autres une figure illustrant l'environnement d'échange de données sécurisées X-Road qui permet un échange de données sécurisé en Estonie (voir Figure 4).

façon sécuritaire et comment offrir des services numériques tout en améliorant la protection de la vie privée[22].

Selon M. Benay, le Canada a encore beaucoup à apprendre de l'Estonie à l'égard de sa plateforme d'échange de données X-Road et il a confié au Comité que des représentants estoniens ont été invités deux fois cette année au Canada pour aider le gouvernement du Canada à créer une plateforme similaire, qui fonctionne dans le contexte des lois, des règlements et des autres contingences du Canada. Selon M. Benay, « La beauté de ce système, s'il va de l'avant » est « que nous pourrons intégrer accessibilité, protection de la vie privée et sécurité. Nous serons aussi en mesure de déterminer comment faire circuler les données au sein du gouvernement du Canada, suivant un ensemble de principes fondamentaux[23]. »

Matthew Anthony, vice-président, Cas d'incident et analyse des menaces chez Herjavec Group, une entreprise offrant des services en matière de cybersécurité, a mis en garde le Comité contre la tentation de prendre l'Estonie comme point de référence pour nos transformations au Canada, parce qu'elle avait certains avantages que le Canada n'a pas[24].

Enfin, Marina Mandal, vice-présidente, Transformation et stratégie bancaires à l'Association des banquiers canadiens (ABC), a mentionné que le livre blanc de l'ABC cite l'exemple de deux pays : l'Estonie et l'Inde. En ce qui concerne l'Estonie, elle a noté que « les similitudes entre les leçons tirées de l'expérience de l'Estonie pour le Canada sont l'importance primordiale de la protection de la vie privée et de la sécurité des données ». Elle a également noté que les similitudes avec l'Estonie s'arrêtent là[25].

22 ETHI, *Témoignages*, 1re session, 42e législature, 19 février 2019, 1555 (Alex Benay, dirigeant principal de l'information du gouvernement du Canada).

23 *Ibid*., 1615.

24 ETHI, *Témoignages*, 1re session, 42e législature, 28 février 2019, 1535 (Matthew Anthony, vice-président, Cas d'incident et analyse des menaces, Herjavec Group).

25 ETHI, *Témoignages*, 1re session, 42e législature, 4 avril 2019, 1545 (Marina Mandal, vice-présidente, Transformation et stratégie bancaires, Association des banquiers canadiens).

PARTIE I — PREMIÈRE ÉTAPE VERS LA NUMÉRISATION DES SERVICES GOUVERNEMENTAUX : L'ADOPTION D'UN CADRE LÉGISLATIF APPROPRIÉ

Plusieurs des témoins entendus par le Comité ont mentionné que pour que le virage numérique des services offerts par le gouvernement du Canada ait du succès, il faut d'abord s'assurer qu'un cadre législatif approprié soit en place.

A. Modernisation des lois relatives à la protection des renseignements personnels

M[me] Cavoukian a affirmé que les lois canadiennes en matière de protection des renseignements personnels sont « vraiment dépassées » et qu'une mise à jour est de mise[26].

> J'appuie totalement le commissaire Daniel Therrien, qui demande au gouvernement fédéral une mise à jour de la LPRPDE [*Loi sur la protection des renseignements personnels et les documents électroniques*], par exemple, qui remonte au début des années 2000. Il a dit également que nous devons ajouter à la nouvelle loi la protection de la vie privée dès l'étape de la conception, car après tout, elle a été intégrée dans le Règlement général sur la protection des données. Nous avons besoin de nouveaux outils. Nous devons agir en amont. Il nous faut déterminer les facteurs de risque et contrer les risques.
>
> […]
>
> Il est absolument essentiel de mettre les dispositions à jour. Il est indispensable de donner au commissaire les pouvoirs dont il a besoin, mais qu'il n'a pas présentement. J'ai été commissaire à la protection de la vie privée pendant trois mandats, et je peux dire que j'avais le pouvoir de rendre des ordonnances. J'y ai rarement eu recours, mais c'est ce qui me permettait d'arriver à une résolution informelle avec des organismes, des ministères qui ne respectaient pas les dispositions sur la protection de la vie privée. C'était une bien meilleure façon de travailler.
>
> J'avais le bâton. Si je devais rendre une ordonnance, je pouvais le faire. C'est ce qu'il manque au commissaire Therrien[27].

Michael Geist, titulaire de la Chaire de recherche du Canada en droit d'Internet et du commerce électronique de la Faculté de droit de l'Université d'Ottawa a comparu en même temps que M[me] Cavoukian. Selon lui, les services gouvernementaux numériques

26 ETHI, *Témoignages*, 1re session, 42e législature, 29 janvier 2019, 1635 (Ann Cavoukian).

27 *Ibid*.

feront intervenir un écosystème beaucoup plus complexe qui s'étend au-delà des questions liées à la pertinence de la *Loi sur la protection des renseignements* (LPRP) à l'ère numérique, qui s'applique à la collecte et l'utilisation des renseignements personnels par des institutions gouvernementales fédérales[28]. En raison du chevauchement entre les régimes public et privé, entre les divers paliers de gouvernement et entre affaires intérieures et étrangères, il a affirmé que le gouvernement canadien devrait mener une évaluation globale qui reconnaît que la prestation de services gouvernementaux numériques va impliquer plus d'une loi ou règlement[29]. Il a néanmoins identifié trois lacunes de la *Loi sur la protection des renseignements personnels* qui, selon lui, méritent d'être corrigées :

1. La LPRP a désespérément besoin d'un mandat pour l'éducation au public et la recherche comme le commissaire l'a fait au niveau de la sensibilisation à l'égard de la LPRPDE[30].

2. La LPRP est loin de répondre aux normes d'une loi moderne sur la protection des renseignements personnels. Le gouvernement devrait être soumis à des limites similaires à celles applicables au secteur privé en matière de collecte de renseignements et tenu de ne recueillir que les renseignements strictement nécessaires à ses programmes et activités[31].

3. La LPRP devrait exiger plus de transparence et imposer au gouvernement, comme c'est maintenant le cas dans le secteur privé sous la LPRPDE, des règles de notification en cas d'atteinte à la sécurité des données et une obligation de publier des rapports de transparence[32].

M. Therrien a de son côté noté que ce qui peut être un obstacle au partage des données entre ministères se trouve aux articles 4 à 8 de la LPRP et que ces règles devraient être réexaminées en vue d'améliorer les services gouvernementaux à l'ère du numérique. Il a rajouté que toute nouvelle mesure législative conçue pour faciliter l'administration de services gouvernementaux numériques doit respecter la vie privée comme un droit de la

28 *Ibid*., 1545 (Michael Geist, titulaire de la Chaire de recherche du Canada en droit d'Internet et du commerce électronique, Faculté de droit, Université d'Ottawa).

29 *Ibid*. Par exemple, ces changements pourraient affecter la LPRP, la *Loi sur la protection des renseignements personnels et des documents électroniques* (LPRPDE), les accords commerciaux contenant des règles sur la localisation et le transfert des données, les politiques en matière de gouvernement ouvert et les normes du secteur privé et les technologies émergentes.

30 *Ibid*.

31 *Ibid*., 1550.

32 *Ibid*.

personne. Il a réitéré les recommandations faites par le Commissariat à la protection de la vie privée du Canada (CPVP) à l'égard de la modernisation de la LPRP en 2016 et en a rajouté une : adopter dans le secteur public le concept de la protection de la vie privée dès la conception[33]. Il a répété qu'il est essentiel d'examiner très attentivement le cadre juridique dans lequel les données seront échangées d'un ministère à l'autre ou dans lequel un ministère sera en mesure de réutiliser des données recueillies par un autre ministère. Sur le plan technologique, il a indiqué que les banques de données ne devraient pas pouvoir communiquer entre elles, à moins qu'une loi les autorise à le faire[34].

M. Therrien a aussi mentionné que le CPVP devrait avoir un rôle et des pouvoirs similaires à ceux dont dispose l'autorité estonienne responsable de la protection des données, qui a un rôle proactif explicite, peut rendre des ordonnances contraignantes, demander l'ouverture de poursuites criminelles et imposer des amendes lorsque des données sont traitées de façon non conforme à la loi[35].

Enfin, M. Therrien a souligné que si des lois sont modifiées pour faciliter la mise en œuvre de services gouvernementaux numériques, le CPVP devrait être consulté. Le CPVP est prêt à jouer un rôle proactif à l'égard des services gouvernementaux numériques, à fournir des conseils aussitôt que possible et à jouer un rôle de surveillance une fois les systèmes adoptés. Cependant, il doit avoir les pouvoirs juridiques nécessaires pour assumer ce rôle[36].

M. Eaves a rappelé qu'en Estonie, avant de commencer à se pencher sur la composante technique de leurs systèmes, les Estoniens ont fait beaucoup de travail pour adapter leurs lois sur la protection des renseignements personnels à la réalité du XXIe siècle et pour créer des systèmes de journaux et de vérifications qui permet aux citoyens de voir qui a accès à leurs données, poser des questions sur la légitimité des accès et interpeller les autorités à cet égard[37].

M. Benay a noté qu'un conseil nouvellement créé, le Conseil d'examen de l'architecture, examine tous les grands projets gouvernementaux sous l'angle de la vie privée. Il a également noté que son organisation a des discussions avec le CPVP sur de potentiels

33 ETHI, *Témoignages*, 1re session, 42e législature, 31 janvier 2019, 1535 (Daniel Therrien).

34 *Ibid*., 1600.

35 *Ibid*., 1540.

36 *Ibid*., 1610.

37 ETHI, *Témoignages*, 1re session, 42e législature, 7 février 2019, 1555 (David Eaves).

obstacles législatifs et a estimé que ce dialogue va s'intensifier à mesure que vont augmenter les services numériques[38].

M. Benay a aussi affirmé que son organisation travaille étroitement avec le ministère de la Justice, ainsi qu'avec Innovation Sciences et Développement économique Canada afin de satisfaire l'obligation imposée au Secrétariat du Conseil du Trésor (le Comité d'examen de l'architecture intégrée) de cataloguer les modifications législatives potentiellement requises[39]. M. Benay a noté que son organisation s'est donnée deux ans pour passer en revue certaines lois qui pouvaient exercer des contraintes par rapport à l'échange d'information[40]. Il a souligné que dans le cadre de ce processus de révision, l'organisation qu'il dirige doit aussi examiner plusieurs ententes de partage de données entre les ministères qui existent[41].

Pour Aaron Snow, dirigeant principal du Service numérique canadien, la voie législative est souvent la plus lente et la plus fastidieuse des solutions et elle peut entraîner des conséquences imprévues. Il a donc argué qu'il faut plutôt aspirer à l'unité de gouvernance la plus petite et la plus rapide qui soit, dans la mesure du possible, pour éviter de se lancer dans un processus de création et de modification des lois[42]. M. Snow, a expliqué que le Service numérique canadien est une nouvelle équipe de prestation de services au sein du Conseil du trésor, dont le mandat est de fournir aux ministères fédéraux une aide pratique qui permet d'accélérer, de simplifier et de rendre plus accessibles et sécuritaires les services numériques et d'appuyer le développement des capacités des ministères à concevoir et à effectuer une prestation de service modernisée[43].

38 ETHI, *Témoignages*, 1re session, 42e législature, 19 février 2019, 1615 (Alex Benay).

39 *Ibid*., 1640.

40 *Ibid*. Le 12 avril 2019, le Comité a reçu du Secrétariat du Conseil du Trésor du Canada (SCTC) un document intitulé « Stratégie de services – répertoire législatif », qui « donne un aperçu préliminaire des dispositions législatives régissant la manière dont les ministères peuvent partager des renseignements, y compris avec d'autres ministères, provinces et tierces parties ». Le Comité a reçu en même temps des réponses écrites du SCTC dont l'objectif est de compléter les réponses fournies oralement par ses représentants le 19 février 2019.

41 *Ibid*., 1650.

42 *Ibid*., 1640 (Aaron Snow, dirigeant principal, Service numérique canadien).

43 *Ibid*., 1540.

B. Protection de la vie privée dès la conception, minimisation des données et consentement

En plus de la modernisation des lois relatives à la protection des renseignements personnels, plusieurs témoins ont discuté de concepts importants en matière de protection des renseignements personnels, dont la protection de la vie privée dès la conception, la minimisation des données et le consentement. Certains ont aussi partagé leur vision du modèle idéal de gouvernement numérique.

1. Protection de la vie privée dès la conception

M[me] Cavoukian a noté que la protection de la vie privée dès la conception est un modèle à somme positive qui permet de réaliser deux gains positifs : la protection des renseignements personnels et la sécurité de ces derniers d'une part, et l'innovation technologique d'autre part[44]. Ce cadre de protection intégrée de la vie privée est fondé sur une intégration proactive de toutes les mesures de protection de la vie privée nécessaires dans l'élaboration des opérations et des politiques à tous les niveaux de services et en matière d'utilisation des données[45]. Selon elle, ce principe, qui contrairement à l'adoption ou la modification des lois qui peut être lente, doit être utilisé comme un moyen proactif de prévenir les préjudices[46].

M[me] Cavoukian a affirmé que la protection des renseignements personnels dès la conception doit également faire partie intégrante du développement des technologies utilisées par le gouvernement fédéral. Par exemple, elle a noté à l'égard de la chaîne de blocs que cette technologie ne garantit pas l'anonymat, qu'elle peut avoir des côtés négatifs et qu'elle a déjà été piratée dans le passé. Pour qu'elle soit efficace, elle doit être mise en place en intégrant la protection des renseignements personnels dans la technologie dès le départ[47].

M. Therrien a de son côté indiqué que la protection des renseignements personnels dès la conception devrait être appliquée sur le terrain par la bureaucratie et les ministères

44 ETHI, *Témoignages*, 1re session, 42e législature, 29 janvier 2019, 1540 (Ann Cavoukian).

45 *Ibid*.

46 *Ibid*., 1600.

47 *Ibid*., 1615.

dans le cadre de la prestation de services[48]. Il a aussi discuté de l'importance de ce concept en matière d'intelligence artificielle.

> La protection de la vie privée dès la conception vise à faire en sorte que l'intelligence artificielle soit utilisée de façon à ce que l'information qui alimente le système ait premièrement été obtenue légalement, deuxièmement, soit fiable et, troisièmement, n'entraîne pas de discrimination pour des motifs interdits et soit fondée sur des facteurs d'analyse objectifs[49].

M. Therrien a aussi illustré l'application de ce principe en discutant du droit à la vie privée comme un droit de la personne.

> Quand je dis que la vie privée est un droit fondamental, il s'agit d'un concept qui devrait être reconnu non seulement par la loi, mais aussi par les instances gouvernementales qui, jour après jour, mettent en place des systèmes de collecte de données et d'administration de programmes publics, technologiques ou autres […] Si nous avons le choix entre offrir un service d'une façon qui met en danger la vie privée et offrir ce même service d'une autre façon tout aussi efficace, mais qui, elle, respecte la vie privée, le concept de protection de la vie privée dès l'étape de la conception nous dit que nous devrions choisir la deuxième option[50].

2. Minimisation des données, dépersonnalisation et consentement

M^me^ Cavoukian a souligné que la minimisation des données est un concept clé dans le monde de la protection de la vie privée et permet aussi d'obtenir de multiples gains simultanément[51].

En matière de dépersonnalisation des données, M^me^ Cavoukian a utilisé son expérience comme consultante pour Sidewalk Labs (SWL) pour offrir un exemple concret de l'importance de ce concept. Elle a expliqué avoir été approchée pour aider SWL à intégrer la protection de la vie privée dès la conception dans la future ville intelligente qui pourrait voir le jour à Toronto. Dès le départ, elle a insisté sur le fait que les données recueillies dans cette future ville intelligente devaient être anonymisées à la source. Plus tard, SWL a dévoilé qu'elle créerait une « fiducie civile des données » qui pourrait être composée de SWL, de divers niveaux de gouvernements impliqués et de diverses sociétés s'occupant de propriété intellectuelle. SWL a alors indiqué ne pas être en mesure de garantir la dépersonnalisation. Après cette annonce, M^me^ Cavoukian a quitté

48 ETHI, *Témoignages*, 1re session, 42e législature, 31 janvier 2019, 1620 (Daniel Therrien).

49 *Ibid*., 1640.

50 *Ibid*., 1630.

51 ETHI, *Témoignages*, 1re session, 42e législature, 29 janvier 2019, 1540 (Ann Cavoukian).

son poste de consultante. Elle travaille maintenant avec Waterfront Toronto pour faire avancer les choses. Selon elle, dès qu'on laisse la décision aux entreprises, il est certain que les données recueillies ne seront pas dépersonnalisées à la source[52].

Quant à la quantité de données recueillie par un gouvernement, M[me] Cavoukian a souligné qu'il est loin d'être préférable d'avoir plus de données. Le gouvernement ne devrait utiliser les données recueillies que pour un but donné, à moins d'avoir obtenu un consentement supplémentaire. Même lorsque l'intention d'un gouvernement est bonne (p.ex. utiliser des renseignements personnels pour sensibiliser les gens à l'existence de fonds qu'ils pourraient recevoir), il ne faut pas s'écarter de la norme, puisqu'il est entièrement possible que les citoyens ne désirent pas que leur gouvernement utilise des données recueillies pour un but précis à des fins de sensibilisation[53]. Elle a rappelé que la protection des renseignements personnels est une question du contrôle que les gens ont à l'égard de l'utilisation de ces données. Dès que le gouvernement élargit la portée de son action parce qu'il estime qu'il sait mieux que quiconque ce qu'il faut faire, cela peut selon elle entraîner le gouvernement dans une voie de surveillance inappropriée[54].

M[me] Cavoukian a souligné que les gens ne fournissent pas leurs renseignements personnels pour que le gouvernement les utilise à sa guise; ils les fournissent pour une raison précise telle payer leurs impôts et le gouvernement ne peut pas utiliser ces renseignements personnels comme bon lui semble[55]. Il s'agit du principe de la spécification des finalités et de la limitation de l'utilisation qui, selon elle, est fondamental à la protection des renseignements personnels[56].

Concernant le consentement relatif à la collecte et l'utilisation des renseignements personnels et la surutilisation des données, M. Geist a affirmé que « nos normes de consentement sont devenues tellement polluées par les normes peu élevées de la LPRPDE que peu de gens ont confiance en ce que signifie le consentement à ce moment-ci ». Il a suggéré de trouver des mécanismes pour que le consentement explicite soit vraiment explicite et éclairé[57]. À l'égard du problème de surutilisation des données, il a indiqué :

52 *Ibid*., 1610.

53 *Ibid*., 1625.

54 *Ibid*.

55 *Ibid*., 1645.

56 *Ibid*.

57 *Ibid*., 1640 (Michael Geist).

> Je pense que vous devez veiller à ce que les gouvernements, comme les entreprises, reconnaissent qu'ils causent un tort considérable à l'écosystème de l'information lorsqu'ils utilisent les données de façon trop agressive, ce qui a pour effet, à terme, de saper la confiance du public, non seulement à leur égard, mais aussi à l'égard des gouvernements en général[58].

M. Therrien a lui aussi noté l'importance pour le gouvernement de ne recueillir que les renseignements dont il a vraiment besoin, même si l'information pourrait être considérée du domaine public.

> Il faut être prudent avant de considérer des renseignements comme étant publics. En effet, comme vous venez de le dire, il est quand même possible d'identifier l'individu qui est associé au véhicule, son comportement, et ainsi de suite. Donc, même si les renseignements sont soi-disant publics, il faut se demander si ce sont néanmoins des renseignements personnels et quelle est l'autorité du ministère en question pour colliger les renseignements. Cela se fait ministère par ministère. Même si ces renseignements sont du domaine public, le fait de les recueillir doit être lié à un mandat du ministère en question. C'est une condition très importante prévue dans la loi actuelle. Elle pourrait être renforcée, selon certaines recommandations que nous avons faites en vue de modifier la LPRP[59].

M. Vickery a indiqué que minimiser la quantité de renseignements personnels recueillis par le gouvernement est aussi bénéfique du point de vue de la cybersécurité[60]. Jason Kint, chef de la direction chez Digital Content Next, a suggéré que lorsqu'une personne est en ligne, ses attentes devraient être les mêmes que lorsqu'elle achète quelque chose au magasin, c'est-à-dire qu'on ne lui demande pas des renseignements qui ne sont pas indispensables[61].

Amanda Clarke, professeure adjointe de l'École d'administration publique et de politique gouvernementale de l'Université Carleton, a de son côté noté qu'il fallait adopter une approche réaliste à l'égard de la capacité des citoyens de donner leur consentement éclairé, notant qu'il a été démontré qu'il faudrait environ 76 jours de travail pour qu'une personne moyenne puisse lire toutes les politiques sur la protection des renseignements personnels numériques qu'elle accepte en une année[62]. Elle a également abordé les enjeux liés à la gestion de données sous l'angle du consentement, en indiquant qu'il faut se demander comment combiner les données, si les citoyens veulent vraiment que l'État

---

58 *Ibid*., 1650.

59 ETHI, *Témoignages*, 1re session, 42e législature, 31 janvier 2019, 1550 (Daniel Therrien).

60 ETHI, *Témoignages*, 1re session, 42e législature, 5 février 2019, 1655 (Chris Vickery).

61 *Ibid*., 1700 (Jason Kint, chef de la direction, Digital Content Next).

62 ETHI, *Témoignages*, 1re session, 42e législature, 7 février 2019, 1540 (Amanda Clarke).

communique directement avec eux et dans quelle mesure ils souhaitent que les ministères puissent avoir accès à leurs renseignements[63].

3. Modèle idéal de gouvernement numérique

Selon M. Benay, le modèle idéal de gouvernement numérique offrirait des services numériques aux Canadiens sur la plateforme technologique de leur choix ou en personne à un comptoir Service Canada, dans un système mis au point en collaboration avec les citoyens qui intégrerait dès sa conception toutes les exigences liées à la protection de la vie privée et l'accès à l'information. Il aimerait aussi offrir un système privilégiant l'interopérabilité entre divers paliers de gouvernement[64].

Selon M. Snow, le modèle idéal de gouvernement numérique serait :

- entièrement transparent et permettrait de comprendre comment le service est dispensé, les étapes qu'il comporte et comment le tout fonctionne;
- souple et adaptable[65].

M. Snow a mentionné que le Service numérique canadien tente d'appliquer les cinq principes suivants dans chacun de ses projets :

1. appliquer des pratiques de recherche et de conception qui font passer les gens d'abord et non des règles et des processus, en se concentrant sur les utilisateurs des services du gouvernement;
2. offrir et améliorer continuellement les choses, en maintenant notamment les programmes de correction du système à jour;
3. présumer qu'il y aura des échecs et être en mesure d'y réagir puisque « La cybersécurité moderne nous encourage à raisonnablement supposer que les défaillances et les intrusions se produiront, et de planifier en conséquence »;

63 *Ibid*., 1640.

64 ETHI, *Témoignages*, 1re session, 42e législature, 19 février 2019, 1620 (Alex Benay).

65 *Ibid*. (Aaron Snow).

4. être transparent, en travaillant au grand jour, à la vue de l'équipe et dans la mesure du possible, du public;

5. avoir de solides boucles de rétroaction entre la prestation et la politique, en écoutant les utilisateurs, en travaillant avec eux, en mettant des prototypes fonctionnels devant eux aussi rapidement que possible et en améliorant continuellement les services pour permettre d'apprendre quelles politiques fonctionnent et comment d'autres échouent et la façon de les mettre à jour[66].

Selon M. Anthony, il faut procéder lentement à la numérisation des services gouvernementaux et attendre que la technologie nécessaire, comme l'intelligence artificielle et les commandes d'automatisation, soit prête à mieux nous soutenir dans cette transformation[67]. Il a mentionné les éléments suivants comme étant des concepts importants de la feuille de route de la Stratégie des données pour la fonction publique fédérale :

- définir une stratégie;
- préciser davantage qui est responsable des données;
- définir les normes et les lignes directrices en matière de gouvernance;
- améliorer le recrutement afin de réunir les compétences nécessaires;
- créer des systèmes technologiques à l'appui de la stratégie[68].

4. Aspects éthiques de l'intelligence artificielle et des algorithmes

En ce qui concerne les travaux du groupe numérique 9 (ou D9, qui comprend, en plus du Canada, l'Estonie, Israël, la Corée du Sud, la Nouvelle-Zélande, le Royaume-Uni, l'Uruguay, le Mexique et le Portugal), M. Benay a fait remarquer que le Canada est à l'origine de la déclaration commune sur l'usage de l'intelligence artificielle[69]. Selon lui, les initiatives en matière d'intelligence artificielle du Canada et les outils qu'il développe (comme le catalogue de fournisseurs et un ensemble d'outils appelé « évaluation

66 *Ibid*., 1540 et 1545.

67 ETHI, *Témoignages*, 1re session, 42e législature, 28 février 2019, 1535 (Matthew Anthony).

68 *Ibid*.

69 ETHI, *Témoignages*, 1re session, 42e législature, 19 février 2019, 1555 (Alex Benay).

d'impact algorithmique », mis en place en collaboration partout dans le monde) le place en tête du peloton en cette matière[70].

En ce qui concerne les aspects éthiques de l'intelligence artificielle et des algorithmes, M. Benay a argué que les différents pays procèdent à l'automatisation de leurs services en fonction de leur cadre de valeurs. Au Canada, les directives mises en place par l'organisation de M. Benay portent sur la garantie que ce n'est pas une boîte noire qui prend la décision au nom d'un humain, par exemple[71]. Sur la transparence algorithmique, M. Benay a noté que les algorithmes de gouvernance représentent un nouvel espace et que certains mécanismes — comme le conseil d'examen de l'architecture — sont en place pour aider à s'assurer que les algorithmes traduisent les valeurs canadiennes et que ces valeurs s'appliqueront à l'ensemble du processus, de l'approvisionnement au déploiement[72].

En vertu de ce qui précède, pour que tout virage vers les services gouvernementaux numériques du gouvernement du Canada soit une réussite, le Comité fait les recommandations suivantes :

Recommandation 1 sur la modernisation des lois relatives à la protection des renseignements personnels du Canada :

Que la *Loi sur la protection des renseignements personnels* et la *Loi sur la protection des renseignements personnels et les documents électroniques* soient modernisées en adoptant les recommandations du Comité relatives à ces lois dans les rapports suivants :

- **Rapport 4 — Protéger la vie privée des Canadiens : examen de la Loi sur la protection des renseignements personnels (décembre 2016)**
- **Rapport 12 — Vers la protection de la vie privée dès la conception : Examen de la Loi sur la protection des renseignements personnels et les documents électroniques (février 2018)**
- **Rapport 16 — Aborder les vulnérabilités de la vie privée numérique et les menaces potentielles au processus électoral démocratique canadien (juin 2018)**

70 *Ibid*., 1625 et 1700.

71 *Ibid*., 1700.

72 *Ibid*., 1705.

- **Rapport 17 — Démocratie menacée : risques et solutions à l'ère de la désinformation et du monopole des données (décembre 2018)**

Recommandation 2 sur la minimisation des données :

Que le gouvernement du Canada s'engage à respecter la minimisation des données, à dépersonnaliser tous les renseignements personnels à la source lorsqu'ils sont recueillis à des fins de recherche ou à des fins semblables et à clarifier les règles de consentement concernant l'échange de renseignements personnels entre ministères et agences gouvernementales.

PARTIE II — MESURES VISANT À ASSURER LE SUCCÈS DU PASSAGE AUX SERVICES GOUVERNEMENTAUX NUMÉRIQUES

A. Bâtir la confiance du public en matière de services gouvernementaux numériques

Jerry Fishenden, qui est professeur invité à la Surrey Business School et œuvre au sein du Centre for the Digital Economy de cette école du Royaume-Uni depuis 2014, a noté qu'il était important de s'assurer que le citoyen soit le gardien de ses renseignements personnels et qu'il y ait les accès et les contrôles nécessaires pour décider ce qu'il est disposé à communiquer à différents fonctionnaires[73].

M[me] Cavoukian a relevé deux exemples qui ont érodé la confiance du public envers le gouvernement, selon elle : le fait de ne pas avoir assujetti les partis politiques aux lois relatives à la protection des renseignements personnels et l'appui du Premier ministre du Canada à Statistique Canada dans ses efforts pour obtenir des renseignements financiers très sensibles du public[74]. M. Geist a abondé dans le même sens[75].

M. Geist a ajouté que l'amélioration du régime fédéral en matière de protection des renseignements personnels favoriserait la confiance du public à l'égard des services gouvernementaux, en veillant par exemple à ce qu'il y ait des mesures de protection

73 ETHI, *Témoignages*, 1re session, 42e législature, 27 mars 2018, 0915 (Jerry Fishenden, professeur invité, Centre for the Digital Economy, Surrey Business School, Université de Surrey, Royaume-Uni).

74 ETHI, *Témoignages*, 1re session, 42e législature, 29 janvier 2019, 1655 (Ann Cavoukian).

75 *Ibid*. (Michael Geist)

adéquates et des mécanismes de transparence informant les citoyens de l'état de leurs données et des niveaux d'accès[76].

M. Therrien a noté que puisque les Canadiens craignent en ce moment que leur vie privée ne soit pas respectée, une mise en œuvre graduelle — permettant au gouvernement de démontrer que le système mérite qu'on lui fasse confiance — pourrait rassurer la population[77].

M[me] Clarke a aussi reconnu que le public doit avoir confiance dans le système pour qu'il fonctionne. Elle a suggéré qu'un modèle centré sur la responsabilité à des fins d'apprentissage permettrait d'établir une culture gouvernementale qui respecte la confidentialité tout en permettant d'être plus novateurs dans l'offre de services[78].

Elle a noté le besoin de mener plus de sondages et d'études dans lesquels on demanderait aux gens s'ils accepteraient que leurs données soient utilisées à des fins autres que celles pour lesquelles elles ont été recueillies en présentant une proposition de valeur. Elle a expliqué qu'il faut présenter une proposition de valeur plutôt que demander aux citoyens s'ils veulent qu'on les surveille et qu'on exploite leurs données à mauvais escient et à grande échelle. Il est clair qu'à la question de surveillance, la réponse sera négative, malgré le fait que ce n'est pas ce dont il est question quand on parle de services gouvernementaux numériques[79]. M. Roy a abondé dans le même sens en suggérant qu'un débat public plus large sur le degré d'aisance des citoyens à l'égard du partage des données soit tenu[80].

M[me] Clarke a aussi mentionné que même si tous les Canadiens ne demandent pas au gouvernement d'aller de l'avant avec la mise en place de services gouvernementaux numériques, ils pourraient être favorables à ces transformations si on leur montrait comment il serait facile de formuler une demande de service avec la saisie automatique de tous leurs renseignements personnels, ou à quel point l'organisation des services en fonction des événements de la vie pourrait faciliter leurs interactions avec l'État[81].

M. Eaves a indiqué qu'au Canada, les gens sont disposés à fournir des renseignements au gouvernement fédéral parce qu'ils ne pensent pas nécessairement que le

---

76 *Ibid.*, 1550.

77 ETHI, *Témoignages*, 1re session, 42e législature, 31 janvier 2019, 1600 (Daniel Therrien).

78 ETHI, *Témoignages*, 1re session, 42e législature, 7 février 2019, 1650 (Amanda Clarke).

79 *Ibid*., 1700.

80 *Ibid*., 1605 et 1615 (Jeffrey Roy, professeur, School of Public Administration, Dalhousie University).

81 *Ibid*., 1640.

gouvernement possède la compétence voulue pour faire des liens à partir de ces renseignements et créer un profil d'eux[82]. Il existe un genre de contrat social entre le gouvernement et les Canadiens voulant que l'utilisation de leurs renseignements personnels soit limitée. Par conséquent, il est d'avis qu'il faudra avoir une discussion intentionnelle au Canada sur l'aspect que pourrait prendre un nouveau contrat social entre le gouvernement et les citoyens dans un gouvernement numérique. Par exemple, en Estonie une partie importante du contrat social est le fait que l'individu qui fournit des renseignements à l'État peut, en échange, voir qui a accès à ses renseignements, pourquoi on les a consultés et dans le cas où l'accès paraît inapproprié, porter plainte[83].

Il a également argué que la participation volontaire du public est nécessaire pour que le passage des services gouvernementaux vers le numérique fonctionne[84]. M. Eaves a ajouté que le virage numérique ne devrait pas mener à la création d'un système à deux vitesses ou les mieux nantis, qui n'ont pas souvent l'occasion d'interagir avec l'État, fournissent peu d'information et sont moins bien connus du gouvernement alors que les plus nécessiteux, qui sont marginalisés et peuvent moins se protéger, doivent communiquer avec l'État de grandes quantités de données[85].

En ce qui concerne l'idée selon laquelle l'amélioration des services gouvernementaux et la protection des renseignements personnels seraient contradictoires, M. Benay a fait valoir qu'en raison des progrès technologiques qui permettent d'intégrer les mesures de protection des données personnelles aux solutions lors des étapes de conception et de développement, ces deux idées ne s'opposent pas[86].

Son organisation a pris des mesures pour promouvoir les services numériques et renforcer la protection des données personnelles des Canadiens, comme :

- l'adoption de normes numériques visant à aider les ministères et les organismes à créer de meilleurs services pour les Canadiens;

- l'élaboration de meilleures règles et lignes directrices pour aider les ministères et organismes à faire la transition à l'ère numérique.

82 *Ibid*., 1555 (David Eaves).

83 *Ibid*., 1620.

84 *Ibid*., 1630 et 1655.

85 *Ibid*.

86 ETHI, *Témoignages*, 1re session, 42e législature, 19 février 2019, 1530 (Alex Benay).

Selon M. Benay, ces mesures appuient les normes ouvertes et les logiciels ouverts, les principes relatifs à l'« infonuagique d'abord » et les principes de la collecte éthique des données et de la sécurité de ces dernières. Les changements apportés permettraient également de mieux travailler à l'échelle du gouvernement en assurant une meilleure fusion entre la technologie et les politiques et en favorisant le dialogue dès le début du processus d'approvisionnement[87].

Selon M. Benay, ces mesures sont essentielles à l'élaboration à long terme de la politique numérique globale du gouvernement du Canada, dont la priorité est l'intégration de la sécurité et de la protection de la vie privée à l'étape du financement et de la conception des services, des programmes et des opérations du gouvernement[88].

M. Benay a expliqué que son organisation travaillait également sur les chantiers suivants :

- une académie du numérique pour la fonction publique, créée en partenariat avec l'École de la fonction publique du Canada;
- des règles visant à encourager l'acceptation des identités numériques et la confiance à leur égard, en collaboration avec les gouvernements provinciaux et territoriaux et le secteur privé;
- un écosystème de gestion des identités numériques afin d'appuyer leur utilisation pour accéder aux services de toutes les administrations;
- une initiative appelée « Connexion Canada », qui permettra aux utilisateurs dans tout le pays d'accéder aux services du gouvernement en ligne via une identité numérique validée et fédérée;
- une plateforme d'échange numérique pour aider les ministères à partager leurs données entre eux et avec le monde extérieur (semblable à la plateforme X-Road utilisée par l'Estonie);
- un nouveau Conseil d'examen de l'architecture d'entreprise qui regroupe des représentants et des intervenants du domaine des opérations et de la technologie de l'ensemble du gouvernement (sur la sécurité, la protection de la vie privée et des données, les applications, la prestation

87 *Ibid*., 1535.

88 *Ibid*.

de services, la transition vers le nuage, l'intelligence artificielle et les défis de gouvernance, par exemple[89]);

- la possibilité d'offrir aux utilisateurs l'expérience « une fois suffit »: le personnel de l'organisation « examine actuellement les processus opérationnels, les politiques et les lois du gouvernement afin de repérer tout obstacle à la concrétisation de cette vision »;

- une étroite collaboration avec le CPVP pour bénéficier de ses conseils concernant les plans et les initiatives qui visent à faire avancer le gouvernement numérique;

- la création de la première liste de fournisseurs d'intelligence artificielle, qui devaient démontrer qu'ils ont les ressources et les compétences nécessaires et qu'ils ont intégré des principes éthiques à leurs pratiques relatives à l'intelligence artificielle, en collaboration avec Services publics et Approvisionnement Canada;

- un nouveau modèle de recrutement (le « nuage de talents du gouvernement du Canada »), mis à l'essai pour faciliter le processus d'embauche et s'adapter au marché[90].

Selon M. Benay, il est

> essentiel de souscrire au principe fondamental voulant que personne ne soit laissé pour compte dans notre stratégie de service. J'estime qu'il s'agira aussi d'une question de confiance. Il va falloir démontrer que nous sommes capables de remplir nos engagements et que les gens peuvent avoir confiance en leur système, d'où l'importance de faire preuve de transparence dans les services que nous allons offrir et dans les politiques que nous élaborons[91].

En ce qui concerne l'importance d'éduquer la population par rapport à la numérisation des services, M. Benay a noté que les initiatives visant à informer la population prennent de plus en plus d'envergure dans certains pays et qu'il faudra inclure l'aspect éducatif dans les programmes gouvernementaux au fur et à mesure que la société progressera vers le numérique[92]. Il a donné l'exemple de l'Uruguay, où on a littéralement apporté

89 *Ibid*., 1555.

90 *Ibid.*, 1550.

91 *Ibid*., 1625.

92 *Ibid*., 1655.

des tablettes iPad dans les maisons des citoyens pour les informer, leur montrer comment faire affaire avec le gouvernement et leur expliquer les choses à faire et à ne pas faire, par exemple, en cas d'attaque sur leur appareil mobile[93].

Della Shea, vice-présidente, Privacy & Data Governance et chef de la protection des renseignements personnels chez Symcor, a présenté trois principes fondamentaux qui sous-tendent, selon elle, la confiance du public par rapport à la gestion des renseignements personnels :

1. la protection de la vie privée dès la conception et la gérance des données;

2. le rôle de fournisseurs de services de confiance dans un écosystème numérique;

3. un cadre législatif cohérent[94].

En ce qui concerne la notion de protection intégrée dès la conception, M[me] Shea a recommandé de créer des mécanismes de contrôle applicables à la façon dont les gouvernements conçoivent leurs systèmes. Elle a ajouté que la gérance des données et son efficacité passent par une opérationnalisation du modèle de responsabilisation établi en vertu de la réglementation canadienne de la protection des renseignements personnels[95].

Quant au rôle de fournisseurs de services de confiance dans l'écosystème numérique, elle a argué qu'il est essentiel que le gouvernement mette en place un modèle de travail prévoyant des fournisseurs de services et des intermédiaires de confiance dans l'écosystème numérique selon lequel les organisations seraient tenues de respecter une norme uniforme « afin de réduire le plus possible la probabilité de vulnérabilités systémiques, mais, de façon plus générale, afin de susciter la confiance dans l'écosystème numérique et la prestation de services numériques[96] ».

En ce qui a trait au troisième principe, M[me] Shea a insisté sur l'importance pour tous les intervenants du monde numérique, dans le secteur privé comme dans le secteur public,

93 *Ibid*.

94 ETHI, *Témoignages*, 1re session, 42e législature, 4 avril 2019, 1535 (Della Shea, vice-présidente, Privacy & Data Governance et chef de la protection des renseignements personnels, Symcor).

95 *Ibid*.

96 *Ibid*.

de respecter des lois cohérentes et rigoureuses en matière de protection de la vie privée[97].

Enfin, en ce qui concerne la participation des personnes âgées à la société numérique en Estonie, M[me] Hanni a signalé que le gouvernement estonien s'était doté de programmes spéciaux pour les y encourager lorsqu'il a pris le virage numérique[98].

À la lumière des renseignements qui précèdent, le Comité recommande :

Recommandation 3 sur la confiance du public envers le gouvernement :

Que le gouvernement du Canada s'efforce d'informer les Canadiens au sujet du passage prochain au gouvernement numérique et de les faire participer à l'élaboration et au développement de l'infrastructure nécessaire à la prestation des services gouvernementaux numériques.

B. Changement de culture dans la fonction publique

M[me] Hänni a souligné que la mise en place d'un gouvernement numérique n'est pas tant une question de technologie qu'une question d'innovation et de coopération novatrice entre différents ministères. Elle a indiqué que pour avoir un bon système de gouvernement numérique il faut apporter des changements radicaux aux attitudes des fonctionnaires et éliminer les cloisons au sein de l'administration gouvernementale en plus d'assurer la collaboration entre toutes les organisations[99].

M. Therrien a indiqué qu'avant de mettre en œuvre des systèmes à plus grande échelle, les hauts fonctionnaires du gouvernement devraient adopter une attitude qui consiste à veiller à ce que des mesures de sécurité soient déployées avant la mise en œuvre des systèmes afin d'éviter des cas comme celui de Phénix, où de hauts fonctionnaires auraient délibérément décidé de ne pas surveiller étroitement l'accès aux renseignements personnels dans le système parce que ça aurait été coûteux et aurait entraîné des retards[100].

Pour sa part, M[me] Clarke a souligné les tensions qui peuvent exister entre le gouvernement numérique et la tradition du gouvernement. Alors qu'on entend souvent

97 *Ibid*.

98 ETHI, *Témoignages*, 1re session, 42e législature, 22 mars 2018, 1000 (Liia Hänni).

99 *Ibid*., 1010.

100 ETHI, *Témoignages*, 1re session, 42e législature, 31 janvier 2019, 1555 (Daniel Therrien).

que les fonctionnaires du gouvernement fédéral ne sont pas suffisamment conscients de l'importance de la protection des renseignements personnels, M^me^ Clarke a plutôt entendu un autre son de cloche dans le cadre de ses travaux, soit que certains fonctionnaires font preuve d'excès de zèle, ce qui peut directement restreindre la portée de l'innovation et l'amélioration des services gouvernementaux, et nuire à l'efficacité des activités quotidiennes du gouvernement[101].

M^me^ Clarke a aussi souligné qu'il est de plus en plus important de réaliser des analyses de politiques transversales qui s'appuient sur des données provenant de nombreux ministères, mais que les lois actuelles, ainsi que les régimes de responsabilisation verticale et les stratégies ministérielles de gestion de l'information favorisent le cloisonnement des données dans la fonction publique. Elle a recommandé une approche plus équilibrée à l'égard de la protection des renseignements personnels et de la sécurité afin d'éviter les pertes d'efficacité qui peuvent avoir lieu lorsqu'on accorde une trop grande priorité à ces sujets[102].

Elle a aussi souligné que le modèle Westminster de Parlement est à l'origine de certaines tensions qui découlent de l'opposition entre les structures verticales de reddition de comptes et le modèle horizontal de plateforme gouvernementale, qui est de plus en plus préconisé. À son avis, ces difficultés peuvent être surmontées. Il faudrait se pencher sur les modèles de responsabilisation horizontale ou de responsabilité partagée si l'on veut déployer des services gouvernementaux numériques à plus grande échelle[103]. M. Eaves a abondé dans le même sens[104].

M. Eaves a ajouté que les défis techniques d'édification de l'infrastructure liée aux services gouvernementaux numériques seront moins grands que les défis en matière de gouvernance. Il a suggéré que trouver le service essentiel, qui aurait le plus d'impact sur les Canadiens et dont la simplification créerait le plus d'intérêt pour la cause, pourrait permettre de collecter les données nécessaires des différents paliers dans un projet pratique et réel[105].

Selon M. Snow, le changement de culture est un lent processus, qui ne se produit habituellement pas au moyen d'une seule directive selon laquelle tout le monde doit commencer à se comporter et à penser différemment en même temps. Son succès se

---

101 ETHI, *Témoignages*, 1re session, 42e législature, 7 février 2019, 1530 (Amanda Clarke).

102 *Ibid*.

103 *Ibid*., 1640.

104 *Ibid*., 1615 (David Eaves).

105 *Ibid*., 1605.

mesure plutôt en observant si les méthodes, pratiques ou outils mis en place pour réaliser un projet donné sont utilisés pour réaliser un autre projet[106].

M[me] Shea a argué que la feuille de route de la stratégie en matière de données publiée l'automne dernier pour la fonction publique « présente une vision globale et permettrait de surmonter le cloisonnement des procédures et d'exploiter l'atout précieux que sont les données » et a invité le gouvernement à

> concevoir un modèle de maturité qui s'adaptera progressivement, qui tient compte non seulement de la protection des renseignements personnels et de la sécurité au fondement même de la numérisation des services gouvernementaux, mais dont la perspective soit une société entièrement numérisée, où toute chose et tout le monde seront branchés sur un écosystème fluide et en expansion constante[107].

À la lumière des renseignements qui précèdent, le Comité recommande :

Recommandation 4 sur le changement de culture dans la fonction publique :

Que le gouvernement du Canada s'efforce d'assurer la collaboration et le partage d'information entre les ministères et les agences gouvernementales en matière d'implantation de services gouvernementaux numériques afin d'assurer le déploiement plus efficace de ces services à grande échelle.

Recommandation 5 sur le partage sécurisé des données :

Que le gouvernement du Canada encourage la connexion des diverses bases de données détenues par des ministères et agences gouvernementales à un réseau fédérateur afin d'assurer le partage sécurisé et contrôlé de données.

C. Garantir l'accès à l'internet

M. Geist a suggéré qu'un facteur important en lien avec la mise en place de normes liées aux services numériques est de s'assurer que tous les citoyens aient accès au réseau pour obtenir les services numériques qui sont créés[108]. Selon lui, pour que le gouvernement passe à un nombre de plus en plus important de services numériques, il est nécessaire d'investir concrètement pour garantir un accès à Internet universel et

106 ETHI, *Témoignages*, 1re session, 42e législature, 19 février 2019, 1630 (Aaron Snow).

107 ETHI, *Témoignages*, 1re session, 42e législature, 4 avril 2019, 1540 (Della Shea).

108 ETHI, *Témoignages*, 1re session, 42e législature, 29 janvier 2019, 1620 (Michael Geist).

abordable pour tous. Tant que ce niveau n'est pas atteint, il estime qu'il faudra assurer un ensemble de services parallèles pour garantir l'accès universel aux services[109].

Le Comité est d'accord avec M. Geist et recommande :

Recommandation 6 sur l'accès à l'Internet :

Que le gouvernement du Canada s'efforce de s'assurer qu'un accès fiable et abordable à Internet soit étendu aux régions rurales et éloignées, même si les services sont numérisés dans les régions déjà desservies.

D. Gouvernance des données des peuples autochtones et impact sur les services gouvernementaux numériques

La question de la souveraineté des données autochtones a été soulevée par M[me] Clarke. Selon elle,

> Cette question soulève des préoccupations tout à fait uniques en ce qui concerne la manière dont le gouvernement du Canada recueille et utilise les données relatives aux peuples autochtones et, en particulier, la façon dont les services sont offerts à ces collectivités. Sachant que ces données ont constamment servi à marginaliser et à opprimer les peuples autochtones, je crois qu'il incombe à votre comité de consacrer du temps à cette question[110].

Le Comité est d'accord avec M[me] Clarke et recommande :

Recommandation 7 sur la gouvernance des données des peuples autochtones :

Que le gouvernement du Canada consulte les peuples autochtones dans le cadre de l'élaboration et du développement des services gouvernementaux numériques.

PARTIE III — AUTRES CONSIDÉRATIONS

A. Identité numérique

Au Royaume-Uni, le programme de carte d'identité a été un échec, selon M. Fishenden, entre autres parce que le Home Office était perçu comme l'arbitre du nouveau registre national d'identité et que les gens allaient devoir stocker toutes leurs données

109 *Ibid*., 1625.

110 ETHI, *Témoignages*, 1re session, 42e législature, 7 février 2019, 1540 (Amanda Clarke).

biométriques et personnelles auprès d'un seul ministère[111]. À son avis, il devrait y avoir des moyens plus efficaces de relier une identité avérée aux différents silos ou dépôts de données afin de confirmer cette identité avec le Service national de la santé et le lien entre cette identité et les dossiers de santé qui y sont reliés, sans que ce lien soit révélé à d'autres ministères sans consentement[112].

Il a souligné qu'au Royaume-Uni :

> On a supposé à tort qu'un seul numéro d'identité pour tout serait une bonne chose à une époque hautement informatisée, alors que dans le modèle estonien, qui est fondé sur une pièce d'identité unique, mais qui maintient la segmentation de vos données […] les citoyens ont toujours le sentiment que ce sont eux, et non pas l'État, qui exercent un contrôle sur leur identité[113].

À cet égard, Andre Boysen, dirigeant principal de l'information chez SecureKey Technologies, a noté que le Canada, les États-Unis, le Royaume-Uni, l'Australie, la Nouvelle-Zélande et de nombreux pays d'Europe s'opposent à l'idée d'une carte d'identité nationale, notamment en raison des dangers liés au regroupement des données en un seul endroit[114].

À propos de ce risque, M. Boysen a expliqué qu'un identificateur unique pour traiter avec le gouvernement est à éviter, parce qu'il permettrait de voir tous les endroits où une personne est allée sur Internet; il mettrait en place un véritable réseau de surveillance. Son organisation a plutôt conçu un système de protection des renseignements personnels à triple barrière pour résoudre ce problème, un service qui requiert des utilisateurs une pluralité d'identificateurs[115].

En ce qui concerne l'utilisation de la chaîne de blocs à cette fin, M. Boysen a fourni l'explication suivante :

> C'est pour vérifier les preuves d'intégrité que nous utilisons les chaînes de blocs. Pour nous, la chaîne de blocs est une méthode pour mettre en place une triple barrière afin de permettre à l'émetteur des données de prouver qu'il en est l'auteur et qu'il s'agit des mêmes données qu'il a fournies à l'utilisateur pour qu'il en fasse état. Le récepteur

111 ETHI, *Témoignages*, 1re session, 42e législature, 27 mars 2018, 0905 (Jerry Fishenden).

112 *Ibid*.

113 *Ibid*., 0925.

114 ETHI, *Témoignages*, 1re session, 42e législature, 28 février 2019,1555 (Andre Boysen, dirigeant principal de l'information, SecureKey Technologies Inc.).

115 *Ibid*., 1625.

> reçoit alors les données en sachant qu'elles n'ont pas été modifiées. Le consommateur peut alors avoir confiance que ces données n'ont pas été partagées indûment[116].

M[me] Cavoukian a, de son côté, souligné que si une identité numérique est bien protégée, qu'elle est chiffrée et que l'accès est restreint, elle peut améliorer l'accès aux services[117].

Ira Goldstein, vice-président directeur, Expansion de l'entreprise, chez Herjavec Group, a argué que l'identité numérique est un élément essentiel de la transformation des services gouvernementaux et que le gouvernement devrait faire preuve de retenue en transformant ses services afin de s'assurer que la protection des données personnelles et la sécurité soient des priorités[118]. Comme exemple de transformation numérique réussie, M. Goldstein a mentionné le système TED de l'Agence du revenu du Canada. Selon lui,

> La numérisation des services gouvernementaux sera bien accueillie par le public si elle fait l'objet d'une gestion et de messages mûrement réfléchis. Cette démarche a pour aspect positif d'améliorer l'accès de groupes historiquement et géographiquement marginalisés, ce qui fait qu'on ne peut ignorer l'occasion qui se présente[119].

Pour sa part, M. Anthony a recommandé au gouvernement de commencer par :

> examiner l'ensemble des différents identificateurs qui sont utilisés actuellement et de choisir des endroits où il pourrait les intégrer à un système d'identification unique qui garantirait une identification de haute qualité pour les transactions qui se font au sein des services gouvernementaux et dans leur environnement[120].

Selon Rene McIver, chef de la sécurité chez SecureKey Technologies, il faut trouver des moyens d'associer les principaux facteurs d'identité pour faire en sorte que les gens sachent que leurs clients sont bien qui ils disent être. Elle a ajouté qu'il faut des réseaux sécurisés et y faire participer les citoyens, dont le contrôle de leurs propres données et la protection de leurs renseignements personnels en garantiront la sécurité[121].

---

116 *Ibid*., 1615.

117 ETHI, *Témoignages*, 1re session, 42e législature, 29 janvier 2019, 1630 (Ann Cavoukian).

118 ETHI, *Témoignages*, 1re session, 42e législature, 28 février 2019, 1530 (Ira Goldstein, vice-président directeur, Expansion de l'entreprise, Herjavec Group).

119 *Ibid*.

120 *Ibid*., 1625 (Matthew Anthony).

121 *Ibid*., 1540 (Rene McIver, chef de la sécurité, SecureKey Technologies Inc.).

M[me] McIver a recommandé d'adopter l'approche de protection des renseignements personnels dite « en triple aveugle », selon laquelle :

> L'organisation qui reçoit les renseignements n'a pas besoin de connaître l'émetteur même de l'information, il lui suffit de savoir qu'elle vient d'une source fiable. L'émetteur n'a pas besoin de savoir qui est l'organisation qui reçoit les renseignements. Et les exploitants de réseau ne sont pas exposés aux renseignements personnels non protégés[122].

En vertu de cette approche, aucun des participants à la transaction n'en voit la totalité. M[me] McIver a noté qu'il s'agit d'une méthode approuvée par des spécialistes de la protection de la vie privée, y compris par le commissaire à l'information et à la protection de la vie privée de l'Ontario. Selon M[me] McIver, les facteurs clés du succès en cette matière sont les suivants :

- s'assurer de l'acceptation et de la confiance des citoyens;
- avoir le potentiel d'atteindre rapidement un grand nombre d'utilisateurs;
- relier ensemble les parties fiables de l'économie numérique, comme la finance, les télécommunications, le gouvernement et le commerce;
- s'assurer de la participation des secteurs privé et public[123].

Selon M. Boysen, une identité est composée de trois éléments qu'il faut maintenir séparés :

1. la question sur l'identité : qui êtes-vous?
2. l'authentification : êtes-vous la même personne que celle qui s'est présentée la première fois?
3. l'autorisation : que suis-je autorisé à faire à l'intérieur de votre service[124]?

M[me] Mandal a noté que « nous sommes toujours liés à un modèle analogique qui repose sur la présentation de documents imprimés pour prouver notre identité dans le cadre des multiples transactions quotidiennes que nous avons avec les services publics, les

122 *Ibid*.

123 *Ibid*.

124 *Ibid*., 1625 (Andre Boysen).

entreprises et les uns avec les autres[125] ». Elle a identifié les trois lacunes majeures suivantes dans le système actuel :

1. il est désuet;

2. même aujourd'hui, les systèmes fondés sur la technologie sont maladroits (il est facile de compromettre la séquence d'identification à deux facteurs utilisée en ligne et les utilisateurs doivent se rappeler de dizaines d'identifiants pour se connecter);

3. l'inefficacité des méthodes de vérification de l'identité freine la croissance économique[126].

Selon M^me^ Mandal, la numérisation des pièces d'identité permet de vérifier l'identité d'une personne électroniquement à l'aide d'une combinaison de systèmes existants et d'outils biométriques plus récents, comme les empreintes digitales ou la reconnaissance faciale[127].

M^me^ Mandal a noté que des mises à jour ont été faites en 2018 à la *Loi sur les banques*, qui permettent expressément aux banques de fournir des services d'identification, de vérification et d'authentification qui vont au-delà de leurs propres besoins opérationnels. Elle a également noté que l'Association des banquiers canadiens a publié l'an dernier un livre blanc « qui expose clairement la voie à suivre pour faire de l'identification numérique une réalité au Canada[128] ». M^me^ Mandal a ajouté que l'ABC a tenu compte des caractéristiques uniques de notre pays, des institutions les plus modernes et de la complexité de l'infrastructure pour élaborer un cadre de référence susceptible de fonctionner ici.

M^me^ Mandal s'est exprimée en faveur d'un modèle fédéré d'identification numérique, qui créerait des liens entre le système fédéral et les systèmes provinciaux de gestion de l'identité. En guise d'exemple de renseignements personnels qui pourraient être fédérés, elle a mentionné les renseignements sur l'assurance sociale et les passeports, qui sont

125 ETHI, *Témoignages*, 1re session, 42e législature, 4 avril 2019, 1530 (Marina Mandal, vice-présidente, Transformation et stratégie bancaires, Association des banquiers canadiens).

126 *Ibid*.

127 *Ibid*.

128 *Ibid*.

gérés par le gouvernement fédéral, et de ceux sur les cartes d'assurance-maladie et les permis de conduire dont les provinces s'occupent[129].

Selon M[me] Mandal, le secteur canadien des banques est idéalement placé pour s'occuper de ce système fédéré d'identification numérique, grâce aux systèmes électroniques interconnectés qui sont déjà en place et au fait que les banques sont déjà tenues de respecter des normes élevées en matière de collecte et de protection des renseignements personnels de leurs clients[130]. Elle a précisé que le système fédéré proposé suppose l'adoption d'une loi permettant aux entreprises et au gouvernement d'accepter l'identification numérique[131].

M[me] Mandal a également souligné l'importance du travail effectué par le Digital Identification and Authentication Council of Canada sur le cadre de confiance pancanadien. L'achèvement prévu de ce cadre de confiance est fixé à l'année prochaine, des projets de discussion étant en cours de production à l'heure actuelle aux fins de commentaires du public[132].

B. Approvisionnement en matière de technologie liée aux services gouvernementaux numériques et gouvernance des renseignements personnels

M[me] Clarke a indiqué qu'une grande partie de la question des services numériques doit porter sur la conception et la livraison des produits, ainsi que sur leur approvisionnement. Elle a suggéré l'utilisation d'une technique, la pensée conceptuelle, qui vise à mener, dès le début, des recherches approfondies sur les utilisateurs futurs d'un service et comment ils l'utiliseront. Une fois ces recherches faites, tout approvisionnement ou conception de services qui doit être réalisé doit être fait en fonction des résultats de ces recherches[133].

Elle a suggéré que l'organisation des services gouvernementaux numériques devrait être faite en fonction des événements de la vie. Elle a expliqué que les citoyens ne souhaitent pas savoir quel ministère fait quoi et ne veulent pas être obligés de visiter une série de sites Web individuels. C'est une question d'optimisation du temps et des ressources : les

129 *Ibid*.

130 *Ibid*.

131 *Ibid*., 1535.

132 *Ibid*., 1545.

133 ETHI, *Témoignages*, 1re session, 42e législature, 7 février 2019, 1610 (Amanda Clarke).

transactions avec l'État ne doivent pas être trop longues. Elle a suggéré qu'une évaluation des besoins des utilisateurs avant de mettre en place tout système horizontal d'une plateforme gouvernementale devrait être faite[134].

M[me] Clarke a aussi souligné que l'État ne s'occupe pas directement de la prestation d'un grand nombre de services numériques gouvernementaux. Selon elle, certaines questions se posent lorsque les interfaces qui appartiennent à des intérêts privés deviennent la seule façon d'avoir accès à des services gouvernementaux ou la manière la plus facile de le faire. M[me] Clarke a suggéré que lorsque des gouvernements sous-traitent la prestation de services numériques à des entreprises privées, ils doivent définir très rigoureusement les données qui peuvent être recueillies, leur utilisation et la monétisation qui peuvent en être faites[135].

Elle a rajouté que le gouvernement devrait s'intéresser aux enjeux liés à la gestion de données et se demander : comment combiner les données, si les citoyens veulent vraiment que l'État communique directement avec eux et dans quelle mesure ils désirent que les ministères aient accès à leurs renseignements. À son avis, au-delà de la question de la protection des renseignements personnels que ces enjeux soulèvent, « il faudra peut-être également concevoir des régimes entièrement nouveaux, pas nécessairement fondés sur la loi, mais plutôt sur les principes à respecter pour l'utilisation des données[136] ».

M. Roy a reconnu certains défis et imperfections associés au travail avec le secteur privé, mais à son avis, il faut faire affaire avec les entreprises technologiques les plus sophistiquées au monde en matière de services gouvernementaux numériques. Ces entreprises ont la capacité requise sur le plan de la sécurité pour garantir la protection des renseignements personnels. Il a aussi indiqué que le secteur privé devrait participer au dialogue sur la protection des renseignements personnels, mais que le gouvernement doit veiller à ce que ces intervenants soient responsables de la façon dont ils participent à l'infrastructure publique et des conséquences connexes[137].

M. Benay a affirmé que des leçons ont été apprises des problèmes reliés au système Phénix et que, dans le cadre de ses activités d'approvisionnement, son organisation tient dans tout le pays des expositions axées sur les utilisateurs qui leur permettent d'essayer différentes technologies et de dire ce qu'ils en pensent. En mettant l'utilisateur au

134 *Ibid*., 1635.

135 *Ibid*., 1540.

136 *Ibid*., 1640.

137 *Ibid*., 1655 (Jeffrey Roy).

centre de ce processus, M. Benay estime que le mécanisme de prise de décisions a été amélioré pour répondre davantage aux besoins réels des gestionnaires des ressources humaines, des administrateurs de la paye et des fonctionnaires ordinaires. Selon lui, toutes les personnes concernées participent à ce processus d'approvisionnement, qui repose aussi sur les principes de la protection de la vie privée[138].

M. Benay a également insisté sur le fait qu'il essaie de s'éloigner du processus habituel d'approvisionnement en collaborant avec les fournisseurs tout au long de la conception de ce processus, à chaque point de contrôle qui a été inséré dans tout le processus[139].

Selon Michael Fekete, associé chez Osler, Hoskin & Harcourt et coprésident du forum légal de l'Association de la technologie du Canada, le gouvernement du Canada accuse un retard par rapport aux gouvernements qui ont déjà adopté l'infonuagique. Ce retard s'expliquerait par le fait qu'à l'heure actuelle, la classification de données impose des exigences de sécurité qui sont incompatibles avec les services infonuagiques. Afin de combler ce retard, M. Fekete a recommandé de s'inspirer de pratiques exemplaires ayant cours à l'étranger, comme le G-Cloud du Royaume-Uni, qui est à la fois un modèle de gouvernement numérique et d'adoption du nuage. Selon M. Fekete, le succès du G-Cloud découle de changements stratégiques apportés délibérément pour favoriser l'adoption de l'infonuagique, par exemple :

- la simplification du régime de classification des données;
- des exigences non prescriptives en matière de sécurité;
- la reddition de comptes pour l'achat de solutions sur mesure;
- l'acceptation d'un contrat de fournisseur « enrobé » de terminologie gouvernementale[140].

M. Fekete a expliqué que les ministères et organismes gouvernementaux du Royaume-Uni sont tenus d'évaluer un service infonuagique en fonction de 14 principes de sécurité infonuagique, qui servent de liste de contrôle pour assurer des mesures de sécurité

138 ETHI, *Témoignages*, 1re session, 42e législature, 19 février 2019, 1605 (Alex Benay).

139 *Ibid*.

140 ETHI, *Témoignages*, 1re session, 42e législature, 21 février 2019, 1545 (Michael Fekete, associé, Technologie, Leader national de l'innovation, Osler, Hoskin & Harcourt S.E.N.C.R.L./s.r.l., Association canadienne de la technologie de l'information).

efficaces sans prescrire pour autant la façon dont un fournisseur de services infonuagiques doit démontrer qu'il s'y conforme[141].

Selon M. Boysen, une seule compagnie ne devrait pas avoir le monopole sur l'approvisionnement des services de technologie numérique utilisés par le gouvernement : un mécanisme ouvert est requis afin d'avoir de multiples fournisseurs[142].

C. Cybersécurité et services gouvernementaux numériques

En matière de cybersécurité des services numériques gouvernementaux, M. Therrien a souligné que les systèmes technologiques sont vulnérables et qu'il devrait y avoir une obligation légale du gouvernement d'appliquer des mesures robustes de protection technologique tels la chaîne de blocs ou le cryptage[143].

D'un point de vue différent, M. Vickery a noté qu'il se méfie de la technologie de la chaîne de blocs, qui n'a pas été suffisamment éprouvée selon lui. Il faudrait, à son avis, que les banques de données ne puissent pas parler la même langue, communiquer entre elles ou regrouper leurs données, mais qu'un intermédiaire puisse le faire. Le gouvernement pourrait ainsi décider que le « traducteur » n'est pas accessible en tout temps et réduire la crainte qu'un individu malintentionné s'introduise dans une banque de données et ait accès à toutes les autres[144].

M. Vickery a aussi indiqué qu'il vaut mieux toujours présumer qu'une atteinte à la protection des renseignements personnels est déjà survenue et de rendre le système tellement segmenté et résiliant, que même dans le cas où une atteinte à la sécurité survient, il est possible de l'identifier rapidement et de minimiser les dommages[145].

M. Vickery a indiqué que le secteur bancaire n'est pas un mauvais choix d'entreprises à qui confier la création et la maintenance d'un système pour la collecte et la protection de données collectées dans le cadre de services gouvernementaux numériques et se porter garant de sa sécurité. L'industrie bancaire est très réglementée et à l'habitude de devoir se soumettre à des audits approfondis, de garder des traces écrites et de faire tout à la lettre. Il a toutefois indiqué qu'il ferait preuve de prudence concernant

141 *Ibid*.

142 ETHI, *Témoignages*, 1re session, 42e législature, 28 février 2019, 1600 (Andre Boysen).

143 ETHI, *Témoignages*, 1re session, 42e législature, 31 janvier 2019, 1555 (Daniel Therrien).

144 ETHI, *Témoignages*, 1re session, 42e législature, 5 février 2019, 1600 (Chris Vickery).

145 *Ibid*., 1655.

l'utilisation des données à d'autres fins et établirait des limites claires à cet égard auprès de toute banque qu'elle implique pour profiter de son expertise et de son infrastructure[146].

M. Benay a affirmé que la sécurité est un ingrédient à incorporer dès le début de la conception des services gouvernementaux numériques et qu'il s'agit d'un élément central de tous les grands projets numériques en cours au gouvernement depuis les 12 derniers mois. À cet égard, il a précisé ne pas préconiser la concentration de l'information gouvernementale dans un seul grand système ou bassin de données[147].

Ruth Naylor, directrice exécutive de la Division des politiques de l'information et de la protection des renseignements personnels à la Direction du dirigeant principal de l'information, a noté qu'en vertu des politiques du Conseil du Trésor, les institutions gouvernementales ont l'obligation de signaler au CPVP et au Secrétariat du Conseil du Trésor les atteintes à la sécurité des renseignements personnels jugées graves. Elle a également noté qu'il y a une collaboration assez étroite entre son organisation et le CPVP pour comparer leurs notes sur ces signalements et que le Secrétariat du Conseil du Trésor met une gamme d'outils à la disposition des institutions pour les aider à déterminer ce qui doit être signalé et à faire rapport en conséquence[148].

M[me] Naylor a mentionné qu'un plan d'action de deux ans est en train d'être élaboré par son organisation et le CPVP. L'objectif de ce plan d'action est de mieux faire connaître la nature des renseignements personnels, en quoi consiste une atteinte et comment il convient de la signaler. Ses efforts sont concentrés sur les responsables des technologies de l'information et de la sécurité pour qu'ils aient le réflexe de reconnaître que des renseignements personnels sont en cause[149].

André Leduc, vice-président, Relations gouvernementales et politiques de l'Association canadienne de la technologie de l'information a témoigné à l'effet que son organisation est d'avis que « si le gouvernement adopte une approche équilibrée et ajuste les

146 *Ibid*., 1620.

147 ETHI, *Témoignages*, 1re session, 42e législature, 19 février 2019, 1605 (Alex Benay).

148 *Ibid*., 1610 (Ruth Naylor, directrice exécutive de la Division des politiques de l'information et de la protection des renseignements personnels, Direction du dirigeant principal de l'information).

149 *Ibid*.

éléments de son système de classification des données et de son cadre de sécurité, ces deux objectifs seront à la fois compatibles et interdépendants[150] ».

En ce qui concerne la technologie 5G, M. Leduc a argué que les réseaux en place actuellement ne suffiront pas pour gérer le volume de données générées par tous les capteurs qui seront présents dans les villes intelligentes, sur les routes, dans les autos automatisées, etc[151]. Il a souligné qu'en matière d'adoption des technologies intelligentes, le Canada se classe au troisième rang mondial selon les Nations unies[152].

M. Fekete a rappelé que la stratégie du gouvernement du Canada sur l'adoption de l'informatique en nuage adoptée l'an dernier oblige les ministères et organismes à suivre une approche structurée de gestion des risques en tenant compte de l'intégration des services infonuagiques dans les services de technologie de l'information qu'ils offrent[153].

Selon M. Anthony, il y a présentement une pénurie générale de compétences pour gérer, développer, essayer, déployer et entretenir en toute sécurité des systèmes logiciels complexes. Il a précisé que cette remarque s'applique à la transformation numérique mondiale[154].

M[me] McIver a exprimé un point de vue unique sur l'utilisation qui peut être faite des données à la suite d'une atteinte à leur sécurité :

> Nous devons en arriver à un point où nous pourrons rendre les données pratiquement inutilisables. Parce que, ce qui compte vraiment, c'est la validation qui vient avec les données. Par conséquent, s'il y a une attaque — qu'il s'agisse de piratage psychologique ou autre — au cours de laquelle les agresseurs s'emparent de données et tentent de quelque manière de les réintroduire dans le système, elles seront rejetées parce qu'elles ne proviennent pas d'une source validée[155].

Angelina Mason, avocate en chef et vice-présidente des affaires juridiques à l'ABC, a argué que l'éducation est un élément important dans la lutte à la cyberfraude. « Nous sensibilisons et informons les consommateurs pour qu'ils connaissent les risques.

---

150 ETHI, *Témoignages*, 1re session, 42e législature, 21 février 2019, 1540 (André Leduc, vice-président, Relations gouvernementales et politiques, Association canadienne de la technologie de l'information).

151 *Ibid*., 1625.

152 *Ibid*., 1630.

153 *Ibid*., 1545 (Michael Fekete); voir Gouvernement du Canada Livre blanc : Souveraineté des données et nuage public.

154 ETHI, *Témoignages*, 1re session, 42e législature, 28 février 2019, 1535 (Matthew Anthony).

155 *Ibid*., 1630 (Rene McIver, chef de la sécurité, SecureKey Technologies Inc.).

Il faudrait aussi échanger de l'information pour trouver des moyens technologiques de bloquer certains types de communications[156]. »

M[me] Mason a noté que le fait d'avoir des données à l'étranger est monnaie courante pour les établissements financiers et les entreprises. Elle a rappelé que la réglementation fédérale de la protection des renseignements personnels exige que les données conservées à l'extérieur du Canada doivent être protégées tout autant qu'elles le seraient au Canada et d'en informer les consommateurs[157].

En ce qui concerne le rôle des banques, John O'Brien, directeur de l'Ingénierie de la sécurité et de la fiabilité au Service numérique canadien, a affirmé ce qui suit :

> Je ne sais pas vraiment comment les banques sécurisent leurs systèmes. De mon point de vue, il serait inopportun de dire qu'elles sont les mieux placées pour protéger la sécurité des Canadiens. J'aimerais beaucoup qu'elles soient plus ouvertes et plus honnêtes à ce sujet, tout comme j'aimerais que Google, Facebook et toutes ces entreprises soient très ouvertes et honnêtes quant à leur façon de faire en matière de sécurité. À ce moment-là, nous pourrions tous collectivement parler de nos positions en matière de sécurité, et je pense que les citoyens canadiens feraient beaucoup plus confiance à toutes les composantes[158].

D. Projet Quayside de Waterfront Toronto

Dans le cadre de son étude relative aux services gouvernementaux numériques, le Comité s'est penché sur le projet Quayside, qui vise à créer une ville intelligente dans un quartier riverain de Toronto. Sidewalk Labs (SWL), une organisation qui appartient à la compagnie Alphabet (dont Google est une filiale) a obtenu le mandat de préparer une proposition offrant un aperçu de cette ville intelligente potentielle qui sera remise à Waterfront Toronto, l'entité qui gère la revitalisation du quartier riverain où le projet de ville intelligente verrait le jour. Ce projet et les défis qu'il comporte a offert un exemple concret de mise en œuvre de services municipaux numériques au Comité.

Le projet a toutefois fait l'objet de vives critiques de la part de certains témoins qui ont comparu devant le Comité dans le cadre du Grand Comité international sur les

156 ETHI, *Témoignages*, 1re session, 42e législature, 4 avril 2019, 1600 (Angelina Mason, avocate en chef et vice-présidente, Affaires juridiques, Association des banquiers canadiens).

157 *Ibid.*, 1605.

158 ETHI, *Témoignages*, 1re session, 42e législature, 19 février 2019, 1635 (John O'Brien, directeur, Ingénierie de la sécurité et de la fiabilité, Service numérique canadien).

mégadonnées, la protection des renseignements personnels et la démocratie qui a eu lieu du 27 au 29 mai 2019.

Shoshana Zuboff, professeure émérite de la Harvard Business School et auteure de *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power* a expliqué ce qui suit :

> C'est un bon signe que nous nous réunissons ce soir dans le magnifique pays qu'est le Canada parce qu'à l'heure actuelle, c'est au Canada que le combat entre le capitalisme de surveillance et la démocratie se livre, plus précisément dans la ville de Toronto. Le capitalisme de surveillance a commencé par la navigation en ligne et il touche maintenant tout ce que nous faisons dans le monde réel. Au moyen des expériences de contagion à très grande échelle menées en ligne par Facebook et du jeu Pokémon GO conçu par Google, le capitalisme de surveillance a expérimenté les façons de rassembler la population en troupeau, ainsi que de régler et de modifier son comportement.
>
> En passant, ces compétences ont maintenant été intégrées à l'application de ville intelligente de Google, qui s'appelle Waze. Or, l'objectif réel, c'est la ville intelligente elle-même. C'est là que le capitalisme de surveillance souhaite prouver qu'il peut remplacer le désordre et la beauté de la gouvernance municipale et de la démocratie par le règne computationnel, qui représente, après tout, une forme de tyrannie absolutiste.
>
> La visée est la ville intelligente. Si le capitalisme de surveillance peut conquérir la ville intelligente, il peut conquérir aussi la société démocratique. Aujourd'hui, le combat se livre à Toronto. Si le Canada donne Toronto à Google, ou plutôt à Alphabet — Sidewalk Labs maintient maintenant avidement qu'elle ne fait pas partie de Google –, l'avenir de la société démocratique au XXIe siècle sera menacé[159].

Jim Balsillie, fondateur et ancien co-président de Research in Motion de même que Président du Centre pour l'innovation dans la gouvernance internationale a indiqué que « les Canadiens, [mènent] actuellement une bataille historique pour l'avenir de notre démocratie contre une mascarade appelée Sidewalk Toronto[160] ». Finalement, Roger McNamee, ancien mentor de Mark Zuckerberg et auteur d'un livre intitulé *Zucked*, a affirmé ce qui suit :

> Je ne laisserais pas Google venir à moins de 100 miles de Toronto. Le problème fondamental ici, c'est l'autonomie gouvernementale et l'autodétermination. Je crois qu'aucune entreprise — pas Google ni qui que ce soit — ne devrait être responsable de gérer nos espaces publics et nos infrastructures municipales. Il y a une limite à ce qu'on peut faire avec un partenariat public-privé, et cela va bien au-delà de cette limite.

159 ETHI, *Témoignages*, 1re session, 42e législature, 27 mai 2019, 1950 et 1955 (Shoshana Zuboff).

160 ETHI, *Témoignages*, 1re session, 42e législature, 28 mai 2019, 0835 (Jim Balsillie).

> […]
>
> Je dirais que je demeure prudent par rapport à la question de la collecte de données. Je crois que les problèmes sous-jacents à la surveillance créent trop de tentations pour les gens. À l'heure actuelle, il est beaucoup trop difficile de surveiller ce que font ces entreprises avec les données après les avoir recueillies. À mon sens, comme on dit souvent au gouvernement, il faut étudier encore davantage tous ces aspects avant d'aller de l'avant[161].

Des représentants de Waterfront Toronto et de SWL ont comparu devant le Comité. Ils ont de leur côté indiqué avoir un engagement envers la protection des renseignements personnels et ont expliqué certaines des mesures qu'ils entendent prendre dans le cadre du projet Quayside afin d'assurer la protection des données recueillies.

Kristina Verner, vice-présidente, Innovation, durabilité et prospérité chez Waterfront Toronto a argué que, même si l'efficacité des lois canadiennes sur la protection de la vie privée par rapport à celles du reste du monde a été démontrée, elles doivent évoluer au même rythme que la technologie. Elle a affirmé que dans le cadre du projet Quayside, Waterfront Toronto traitera la protection de la vie privée au-delà de la lettre de la loi et que le projet reflète les valeurs canadiennes en cette matière[162]. Elle a expliqué que les mesures suivantes seront prises par Waterfront Toronto :

1. conformité avec toutes les exigences législatives et réglementaires qui s'appliquent au projet et intention de suivre les principes de la protection intégrée de la vie privée (le projet ne sera accepté que s'il suit ces principes);

2. aucun traitement préférentiel ne sera accordé à une filiale d'Alphabet, y compris Google, qui lui permettrait de divulguer ou d'utiliser des données personnelles;

3. aucune utilisation des données à des fins publicitaires sans obtenir un consentement exprès;

4. anonymisation des renseignements personnels à la source, à moins que l'on ait obtenu un consentement éclairé et exprès à l'effet contraire pour une fin précise;

---

161 Ibid., 0930 (Roger McNamee).

162 ETHI, *Témoignages*, 1re session, 42e législature, 21 février 2019, 1535 (Kristina Verner, vice-présidente, Innovation, durabilité et prospérité, Waterfront Toronto).

5. efforts pris pour réduire au minimum la collecte de données afin de ne recueillir que celles qui sont requises à des fins limitées et précises;

6. entreposage au Canada des données recueillies pour le projet Quayside[163].

M[me] Verner a aussi rappelé l'engagement de Waterfront Toronto de dépersonnaliser les données à la source (au point de collecte ou au point initial d'hébergement ou de traitement). En ce qui concerne les capteurs d'information prévus dans la ville intelligente, elle a argué que la proposition de Waterfront Toronto est que, dès la collecte d'information, l'image d'une personne serait convertie en une forme suffisamment floue pour empêcher de détermine le sexe, l'âge, les différences sur le plan des capacités, etc. Cette image serait convertie en chiffres et en algorithmes et deviendrait ainsi une statistique, sous-entendant que les risques pour la protection de la vie privée seraient réduits[164].

M[me] Verner a suggéré, toutefois, que si toutes les données étaient ouvertes par défaut, cette situation pourrait défavoriser certaines petites entreprises canadiennes et que cette question devra être abordée lors des prochaines étapes[165].

En ce qui concerne la question de fiducie de données civiques, qui a été proposée dans le cadre du projet Quayside, M[me] Verner a fait valoir que les fiducies de données civiques offrent un modèle de gouvernance possible, mais que les représentants de Waterfront Toronto ont l'intention d'en examiner d'autres, une fois qu'ils auront une meilleure idée de ce qui est envisagé. Elle a précisé que Waterfront Toronto n'est pas intéressée à jouer le rôle de gardien des données ou de surveillant numérique du projet[166].

En ce qui concerne la collecte de données dans l'environnement physique par des caméras et des capteurs, ou « données urbaines », SWL a de son côté proposé la création d'un organisme indépendant chargé de superviser la collecte et l'utilisation des données urbaines, « de manière à protéger l'intérêt public tout en encourageant l'innovation[167] ».

---

163 *Ibid*.

164 *Ibid.*, 1555.

165 *Ibid.*, 1640.

166 *Ibid.*, 1645.

167 ETHI, *Témoignages*, 1re session, 42e législature, 2 avril 2019, 1540 (Dan Doctoroff, , directeur général, Sidewalk Labs)

Dan Doctoroff, le directeur général de SWL a précisé que, par défaut, Sidewalk Labs souhaite que les données urbaines soient ouvertes à tous et qu'elles soient anonymisées. Il a toutefois émis un bémol concernant certaines situations où SWL pourrait faire valoir qu'il est impossible d'en obtenir toute la valeur sans en limiter l'accès davantage, ce qui échapperait à la responsabilité de l'entreprise et serait fait par une fiducie de données civiques en consultation avec les organismes de réglementation de la protection de la vie privée[168].

M. Doctoroff a aussi affirmé que :

> Conformément aux lois et aux valeurs canadiennes en matière de protection de la vie privée, nous avons pris dès le départ des engagements concernant l'utilisation responsable des données, notamment en adhérant aux principes de la protection intégrée de la vie privée, de l'anonymisation et de la minimisation des données et de l'interdiction de vendre des données personnelles provenant de ce projet ou de les utiliser à des fins publicitaires[169].

Questionné sur son modèle d'affaires et sur la manière dont SWL compte être profitable, M. Doctoroff a affirmé que SWL n'a aucune raison de monétiser les renseignements personnels[170].

Le Comité a également entendu le témoignage de Brian Kelcey, vice-président, Affaires publiques du Toronto Region Board of Trade à l'égard du projet Quayside. M. Kelcey a argué que le processus sur lequel se sont entendus Waterfront Toronto et SWL devrait aller de l'avant et que le résultat final devrait dépendre des avantages ou des inconvénients de ce que propose SWL dans son plan de développement[171].

M. Kelcey a présenté les principales recommandations du rapport intitulé *BiblioTech* publié par son organisation au début du mois de janvier 2019 et portant sur la gouvernance des données qui seraient recueillies dans le cadre du projet Quayside :

- la réglementation en matière de données concernant le projet Quayside devrait être gérée par une tierce partie, et non pas par les promoteurs ou les participants du projet;

168 *Ibid.*, 1645.

169 *Ibid.*, 1540.

170 *Ibid.*, 1610.

171 ETHI, *Témoignages*, 1re session, 42e législature, 9 avril 2019, 1605 (Brian Kelcey, vice-président, Affaires publiques du Toronto Region Board of Trade).

- toute donnée du domaine public recueillie à Toronto devrait être conservée par un centre de données public ou un système hôte, ou une fiducie de données, en vertu de la loi et des règlements;

- un bon hôte potentiel pour ce centre de données serait la Bibliothèque publique de Toronto;

- l'application de ces règles devrait relever du commissaire à l'information et à la protection de la vie privée de l'Ontario;

- ces règles devraient être renforcées au besoin et le commissaire devrait avoir le pouvoir d'enquêter sur les infractions aux règles de ce centre de données si nécessaire;

- la Bibliothèque publique de Toronto devrait s'inspirer des approches utilisées dans les bureaux de transfert de technologies des universités et des établissements postsecondaires pour tout effort visant à saisir la valeur de la propriété intellectuelle à partir de ces données;

- les recettes devraient servir à rendre le centre autosuffisant, même si la commercialisation des données était limitée[172].

Selon M. Kelcey, un consensus existe sur la nécessité pour les données du domaine public d'être réglementées par des gouvernements ou des organismes si SWL désire commercialiser les données provenant des capteurs installés à Quayside[173]. Une fois recueillies, les données du domaine public « devraient être conservées indépendamment par une autorité externe, que ce soit le gouvernement, une fiducie ou un organisme approprié[174] ».

En vertu des témoignages entendus à l'égard du projet Quayside, le Comité recommande :

Recommandation 8 sur l'établissement de lignes directrices et de principes pour des projets de ville intelligente :

Que le gouvernement du Canada, en partenariat avec les gouvernements provinciaux, municipaux et autochtones, établisse des principes directeurs relatifs à la protection des

172 *Ibid.*

173 *Ibid.*

174 *Ibid.*, 1610.

renseignements personnels, la cybersécurité et la littéracie numérique dans des projets de ville intelligente.

CONCLUSION

Le Comité a pu constater dans le cadre de son étude que plusieurs avancées en matière de services gouvernementaux numériques sont en cours au sein du gouvernement fédéral.

Plusieurs témoins ont toutefois soulevé des pistes de solutions potentielles visant à permettre au gouvernement du Canada de s'assurer que le déploiement de services numériques soit fait de façon efficace et avec succès.

À la lumière de l'ensemble des témoignages entendus, le Comité reprend certaines de ces pistes de solutions à son compte et les présente sous forme de recommandations. Il tient également à souligner l'importance de s'assurer que le virage vers les services gouvernementaux numériques ne se fasse pas au détriment de la protection des renseignements personnels de la population canadienne.

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
E-Governance Academy	2018/03/22	96
Liia Hänni, experte principale		
Raul Rikk, directeur de programme Cybersécurité nationale		
À titre personnel	2018/03/27	97
Jerry Fishenden, technologue et conseiller gouvernemental		
À titre personnel	2019/01/29	132
Ann Cavoukian Privacy by Design Centre of Excellence, Ryerson University		
Michael Geist, titulaire de la chaire de recherche du canada en droit d'internet et du commerce électronique Faculté de droit, Université d'Ottawa		
Commissariat à la protection de la vie privée du Canada	2019/01/31	133
Lara Ives, directrice exécutive Direction des politiques, de la recherche et des affaires parlementaires		
Gregory Smolynec, sous-commissaire Secteur des politiques et de la promotion		
Daniel Therrien, commissaire à la protection de la vie privée du Canada		
À titre personnel	2019/02/05	134
David Carroll, professeur associé Parsons School of Design, The New School		
Chris Vickery, directeur de la recherche sur les risques cybernétiques UpGuard		

Organismes et individus	Date	Réunion
Digital Content Next	2019/02/05	134
Jason Kint, chef de la direction		
À titre personnel	2019/02/07	135
Amanda Clarke, professeure adjointe et titulaire de la chaire d'excellence en recherches sur les affaires publiques School of Public Policy and Administration, Carleton University		
À titre personnel	2019/02/07	135
David Eaves, conférencier en politiques publiques Digital HKS, Harvard Kennedy School		
Jeffrey Roy, professeur School of Public Administration, Dalhousie University		
Secrétariat du Conseil du Trésor	2019/02/19	136
Alex Benay, dirigeant principal de l'information du gouvernement du Canada		
Ruth Naylor, directrice exécutive Division des politiques de l'information et de la protection des renseignements personnels, Direction du dirigeant principal de l'information		
John O'Brien, directeur Ingénierie de la sécurité et de la fiabilité, Service numérique canadien		
Aaron Snow, dirigeant principal Service numérique canadien		
Association canadienne de la technologie de l'information	2019/02/21	137
Michael Fekete, associé Technologie, Leader national de l'innovation, Osler, Hoskin & Harcourt S.E.N.C.R.L./s.r.l.		
André Leduc, vice-président Relations gouvernementales et politiques		
Waterfront Toronto	2019/02/21	137
Meg Davis, directrice du développement		
Kristina Verner, vice-présidente Innovation, durabilité et prospérité		

Organismes et individus	Date	Réunion
Herjavec Group	2019/02/28	139
Matthew Anthony, vice-président Services de remédiation de sécurité		
Ira Goldstein, vice-président directeur Expansion de l'entreprise		
SecureKey Technologies Inc.	2019/02/28	139
Andre Boysen, dirigeant principal de l'information		
Rene McIver, chef de la sécurité		
Sidewalk Labs	2019/04/02	141
John Brodhead, directeur des politiques et stratégies		
Dan Doctoroff, directeur général		
Micah Lasher, chef des politiques et des communications		
Association des banquiers canadiens	2019/04/04	142
Marina Mandal, vice-présidente Transformation et stratégie bancaires		
Angelina Mason, avocate en chef et vice-présidente, affaires juridiques		
Symcor inc.	2019/04/04	142
Della Shea, vice-présidente Privacy & Data Governance et chef de la protection des renseignements personnels		
Toronto Region Board of Trade	2019/04/09	143
Brian Kelcey, vice-président Affaires publiques		

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.

Di Lorenzo, Julie

Eaves, David

Rubin, Ken

Sack, Cybele

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 96, 97, 132 à 137, 139, 142 à 144, 149, 150, 156, 158 et 159) est déposé.

Respectueusement soumis,

Le président,
Bob Zimmer

Rapport complémentaire sur les villes intelligentes et les droits démocratiques

Nouveau Parti démocratique

Introduction

Dans le cadre de son étude sur la protection des données personnelles dans les services gouvernementaux numériques, le Comité a entendu des témoignages sur une question connexe, en l'occurrence un projet controversé visant à créer une « ville intelligente » dans un quartier riverain de Toronto, qui est mis au point par Sidewalk Labs, une organisation appartenant à la compagnie Alphabet.

Ce projet fait suite à une demande de propositions de Waterfront Toronto, une entité établie conjointement par le gouvernement du Canada, le gouvernement de l'Ontario et la Ville de Toronto pour s'occuper du développement du secteur riverain de la ville, qui recherchait un partenaire d'innovation et de financement pour l'aménagement d'un terrain de 12 acres appelé Quayside.

Depuis l'annonce conjointe de Waterfront Toronto et de Sidewalk Labs, en octobre 2017, lors de laquelle le président exécutif d'Alphabet, Inc., Eric Schmidt, était présent, le projet de « ville intelligente » a semé la controverse; par exemple, un rapport de la vérificatrice générale de l'Ontario a soulevé d'importantes questions au sujet de ce projet, et de nombreux conseillers de Sidewalk Labs et de Waterfront Toronto ont remis leur démission.

Parmi les préoccupations soulevées, mentionnons la protection de la vie privée des résidents, le processus dans le cadre duquel Sidewalk Labs a obtenu la permission d'élaborer un plan directeur en matière d'innovation et de développement, la privatisation d'un espace public, l'incidence possible à long terme du projet sur la capacité d'innovation du Canada, et le modèle d'affaires fondé sur le capitalisme de surveillance de Sidewalk Labs, une organisation appartenant à la compagnie Alphabet.

Le projet se heurte maintenant à une forte résistance de la part d'une coalition de Torontois appelée Block Sidewalk.

Les néo-démocrates recommandent que :

1. le gouvernement du Canada suspende ses engagements envers Sidewalk Labs jusqu'à ce qu'un plan détaillé définitif soit soumis à Waterfront Toronto, à la Ville de Toronto, au gouvernement de l'Ontario et au gouvernement fédéral;
2. tout projet de « ville intelligente » à venir au Canada devrait commencer par une consultation publique visant à déterminer les besoins et les souhaits des résidents;
3. tout projet de ce type devrait toujours viser à répondre à ces besoins et souhaits réels;
4. tout projet de ce type devrait prendre en compte, dans toute la mesure du possible, les commentaires des citoyens et leurs idées quant à sa conception;
5. aucun projet de « ville intelligente » ne devrait en définitive être mis en œuvre afin de poursuivre un modèle d'affaires fondé sur le capitalisme de surveillance.

Préoccupations relatives au processus – Demande de propositions

Dès le départ, de sérieuses réserves ont été exprimées à propos du projet Quayside et du processus ayant donné lieu à la sélection de Sidewalk Labs comme partenaire d'innovation et de financement possible ayant obtenu la permission d'élaborer un plan directeur en matière d'innovation et de développement à l'intention de Waterfront Toronto.

La demande de propositions initiale de Waterfront Toronto, intitulée « Request for Proposals: Innovation and Funding Partner for the Quayside Development Opportunity », a été publiée le 17 mars 2017; on y précisait que la date limite pour présenter une proposition était le 27 avril 2017[1]. Cela correspond à six semaines, ou 30 jours ouvrables.

La mise en œuvre d'un projet de « ville intelligente » est une énorme entreprise, et en fait, le projet dont il est question dans le présent document serait le premier de ce type et de cette portée au Canada. Il soulève des questions complexes, notamment en ce qui concerne la collecte de données et la protection de la vie privée, la gouvernance et la responsabilité démocratique, la propriété intellectuelle et l'utilisation des terres. Comme la vérificatrice générale de l'Ontario l'a indiqué dans son rapport portant sur la vérification de 2018 visant Waterfront Toronto, « les répondants disposaient de 6 semaines pour répondre à une demande de propositions complexe, par comparaison aux 10 semaines qui avaient été accordées aux répondants dans le cas des projets d'art public du quartier des terrains de l'Ouest de la rivière Don[2] ». Dans son rapport, la vérificatrice générale indique également que Waterfront Toronto avait déjà accordé « 11 semaines pour retenir les services d'un gestionnaire de la construction pour la protection contre les inondations dans les terrains portuaires et 25 semaines à un promoteur pour mener un projet de construction d'un immeuble de bureaux unique[3] » dans le cadre d'une demande de propositions. Elle en a conclu que « les répondants n'ont pas eu suffisamment de temps pour répondre à la [demande de propositions] en six semaines[4] ».

Le 21 février 2019, lors d'une réunion du Comité, la directrice du développement de Waterfront Toronto, Meg Davis, a déclaré au Comité que le processus de la demande de propositions a été de 159 jours. Le directeur général de Sidewalk Labs, Dan Doctoroff, a déclaré la même chose au Comité lors de sa comparution, le 2 avril 2019.

Il semblerait que malgré ces affirmations, Waterfront Toronto n'a pas abordé cette question avec la vérificatrice générale de l'Ontario dans le cadre de sa vérification de la rentabilité de l'organisation, et cette dernière a donc déclaré que seulement six semaines ont été accordées pour répondre à la demande de propositions, comme cela est indiqué ci-dessus. Par ailleurs, Waterfront Toronto n'a pas dit qu'elle s'opposait à cette interprétation de la situation dans ses réponses officielles à la vérificatrice générale, qui ont été incluses dans son rapport. Une déclaration du président-directeur général par intérim de Waterfront Toronto, Michael Nobrega, publiée en réponse au rapport de la vérificatrice générale, ne faisait également aucune allusion à la brièveté de la période accordée pour répondre à la

[1] Waterfront Toronto, *Quayside Request for Proposals: Innovation and Funding Partner for the Quayside Development Opportunity*, 17 mars 2017, p. 1. https://waterfrontoronto.ca/nbe/wcm/connect/waterfront/3f21abe9-a5bb-4665-8cd3-322e1e13811f/Waterfront+Toronto+-+RFP+No.+2017-13.pdf?MOD=AJPERES&CACHEID=3f21abe9-a5bb-4665-8cd3-322e1e13811f

[2] Vérificatrice générale de l'Ontario, *Rapport annuel 2018*, « Chapitre 3.15 : Société de revitalisation du secteur riverain de Toronto », p. 761.

[3] Vérificatrice générale, Société de revitalisation du secteur riverain de Toronto, p. 805.

[4] *Ibid*., p. 805.

demande de propositions et rien dans cette déclaration ne remettait en question les conclusions de la vérificatrice générale, selon lesquelles cette période n'avait été que de six semaines[5].

L'un des membres conservateurs du Comité, M. Kent, a fait valoir, lorsqu'il a posé des questions à M. Doctoroff, que les autres parties ayant donné suite à la demande de propositions étaient conscientes qu'elles avaient 30 jours pour présenter leur proposition, comme cela était indiqué dans la demande de propositions initiale visant le site Quayside. M. Doctoroff n'a pas contredit ces propos.

Les néo-démocrates députés estiment que, même si Waterfront Toronto et Sidewalk Labs insistent sur le fait que la période de la demande de propositions était de 159 jours, cette affirmation va à l'encontre de ce qui est indiqué dans leurs propres documents, de l'interprétation des autres répondants, du rapport de la vérificatrice générale de l'Ontario et de la couverture médiatique accordée au processus, et donc, elle n'est pas crédible.

Dans notre régime politique, les fonctions de surveillance précise qu'assume la vérificatrice générale sont essentielles. Il ne suffit pas de contredire tout bonnement le rapport de la vérificatrice générale, surtout après sa publication, comme l'ont fait Waterfront Toronto et Sidewalk Labs. Ce fait a ébranlé notre confiance envers le projet et devrait inquiéter les Torontois et l'ensemble des Canadiens.

Étant donné l'ampleur et la puissance de la société Alphabet, ainsi que les inquiétudes, maintes fois signalées, de la population en ce qui concerne les aspects du projet qui touchent à la technologie et à la gouvernance, il est inacceptable qu'on contredise ainsi le rapport.

En outre, compte tenu de la complexité des projets de « ville intelligente », dont il a été question ci-dessus, et étant donné que Sidewalk Labs a indiqué dans les mémoires présentés à la vérificatrice générale qu'elle voit son engagement envers Toronto comme un projet « devant s'échelonner sur plus d'une vingtaine d'années », la brève période accordée pour répondre à la demande de propositions est en soi inappropriée.

Les néo-démocrates estiment que tout projet de « ville intelligente » devrait comprendre des consultations approfondies et proactives auprès des résidents et une longue période pour élaborer les plans et répondre publiquement aux préoccupations exprimées. Qui plus est, les résidents, les fonctionnaires municipaux et le reste de la population devraient être en mesure de bien comprendre ce à quoi ils consentent, à toutes les étapes du processus.

Enfin, les néo-démocrates ne savent pas exactement si Waterfront Toronto est l'organisation appropriée pour prendre un engagement générationnel, comme le projet à long terme de « ville intelligente », qui comporte beaucoup d'inconnues, étant donné que l'article 13(3) de sa loi habilitante, la *Loi de 2002 sur la Société de revitalisation du secteur riverain de Toronto*, prévoit que le lieutenant-gouverneur en conseil exigera la liquidation de Waterfront Toronto au plus tard en 2028.

Préoccupations relatives au processus – Ingérence politique concernant l'approbation de l'accord-cadre

[5] Waterfront Toronto, *Statement by Waterfront Toronto Interim CEO Michael Nobrega Regarding the Report of Ontario's Auditor General*, 5 décembre 2018. https://waterfrontoronto.ca/nbe/portal/waterfront/Home/waterfronthome/newsroom/newsarchive/news/2018/december/statement+from+waterfront+toronto+regarding+ontario+auditor+general+report

Dans son rapport, la vérificatrice générale indique que Waterfront Toronto « n'a pas consulté adéquatement les ordres de gouvernement au sujet du projet de Sidewalk Labs ». Elle a indiqué qu'au lieu de consulter les ministères provinciaux et fédéraux pertinents et la Ville, « [c]ela faisait l'objet de discussions à un niveau politique supérieur[6] ». Elle a également mentionné que « le conseil s'était fait demander « instamment » par les gouvernements fédéral et provincial d'approuver et d'autoriser l'entente-cadre avec Sidewalk Labs le plus tôt possible », que le conseil lui-même n'avait eu qu'une journée pour examiner et approuver l'accord-cadre, et que l'annonce publique du 17 octobre sur l'approbation de l'accord-cadre par le premier ministre du Canada, la première ministre de l'Ontario, le maire de Toronto et le président exécutif d'Alphabet avait été organisée le 12 octobre, « soit la veille du jour où le conseil a reçu l'entente-cadre finale à des fins d'examen et d'approbation[7] ».

Même si la vérificatrice générale n'a pas fourni plus de détails sur la nature de ces discussions à un niveau politique supérieur, elle a également constaté que la demande de propositions de 2017, qui visait à identifier un partenaire en matière d'innovation et de financement, ne correspondait pas aux objectifs et aux priorités énoncés dans le plan stratégique 2014-2023 de Waterfront Toronto, et que le Comité directeur intergouvernemental de Waterfront Toronto avait lui-même adressé des reproches à l'organisation lors d'une réunion, en novembre 2017, parce qu'on n'avait pas laissé suffisamment de temps au conseil de Waterfront Toronto pour prendre d'importantes décisions[8].

Dans son mémoire au Comité, M[me] Julie Di Lorenzo, qui a déjà été membre du conseil de Waterfront Toronto et ancienne présidente de l'Investment and Real Estate Committee (IREC) et a remis sa démission en raison de la façon dont l'organisation a géré le projet Sidewalk, a exprimé de graves préoccupations à l'égard du processus d'approbation de l'accord-cadre initial d'octobre 2017 et des inexactitudes dans les témoignages présentés par Waterfront Toronto au Comité sur cette question.

Dans sa lettre, elle indique qu'elle a voté contre l'accord-cadre, car son comité, l'IREC, « a examiné chaque article et chaque virgule, et a aidé l'équipe à négocier », comme l'a indiqué M[me] Davis, de Waterfront Toronto, lors de son témoignage devant le Comité, le 21 février[9]. Elle a uniquement reçu l'accord-cadre quatre jours ouvrables avant la réunion du conseil. Ce dernier a approuvé l'accord-cadre sans tenir compte de la recommandation de l'IREC. Comme l'a souligné M[me] Di Lorenzo, normalement, « si le président du principal sous-comité s'oppose à une motion, c'est un motif suffisant pour suspendre toute autre mesure jusqu'à ce qu'on ait au moins effectué une étude approfondie des préoccupations de ce président. Et le fait que la présidente de l'Investment and Real Estate Committee ait voté contre un projet immobilier et d'investissement est une situation extraordinaire[10] ».

M[me] Di Lorenzo a également déclaré que ce que M[me] Davis a prétendu lorsqu'elle a témoigné devant le Comité, soit qu'une seule personne s'est opposée à l'accord-cadre lors de la réunion du conseil, le 16 octobre, est techniquement exact, mais ne constitue pas une interprétation juste de la situation.

---

[6] Vérificatrice générale, Société de revitalisation du secteur riverain de Toronto, p. 762.
[7] *Ibid*., p. 806.
[8] *Ibid*., p. 804.
[9] M[me] Meg Davis, témoignage devant le Comité permanent de l'accès à l'information, de la protection des renseignements personnels et de l'éthique, 21 février 2019.
[10] Julie Di Lorenzo, mémoire présenté au Comité permanent de l'accès à l'information, de la protection des renseignements personnels et de l'éthique, 9 mai 2019, p. 2.
https://www.noscommunes.ca/Content/Committee/421/ETHI/Brief/BR10470671/br-external/DiLorenzoJulie-10049950-f.pdf

M[me] Di Lorenzo a déclaré que deux membres du conseil étaient absents et n'ont pas voté par procuration, et qu'un autre membre s'est abstenu. Comme elle l'a indiqué, « la présidente du principal sous-comité du conseil a voté contre, deux membres étaient absents et un membre du conseil s'est abstenu. Contrairement à la description de l'assemblée donnée par M[me] Davis, dans les faits, le vote du conseil sur la motion témoigne d'une *absence flagrante* de consensus par Waterfront Toronto, le conseil étant de toute évidence divisé et mal informé au sujet d'un accord aussi important et historique et n'ayant pas un délai raisonnable pour examiner et étudier les répercussions de cet accord[11] ».

M[me] Davis a déclaré au Comité que l'Investment and Real Estate Committee a tenu plusieurs réunions à propos de l'accord-cadre avant qu'il soit dévoilé, mais M[me] Di Lorenzo a indiqué que cette affirmation « est trompeuse[12] ». Elle affirme que comme elle était la présidente de ce comité, « ces réunions ne portaient pas sur l'accord-cadre, puisque cet accord n'a pas été accessible avant le long week-end de l'Action de grâces de 2017. Les réunions de l'IREC avant le week-end de l'Action de grâces de 2017 portaient sur différents points opérationnels de Waterfront Toronto, comme le logement abordable, des séances d'information de haut niveau sur l'accord potentiel, mais pas sur l'accord-cadre comme tel[13] ». Ces renseignements sont corroborés par le rapport de la vérificatrice générale, lequel indique que le comité « a obtenu un aperçu des principes et des modalités provisoires de l'entente-cadre environ un mois avant la présentation de celle-ci au conseil pour approbation[14] ».

Comme cela a été mentionné ci-dessus, le projet de « ville intelligente » de Sidewalk Labs représente un engagement générationnel pour la Ville de Toronto et les Canadiens. Les irrégularités observées dans le processus d'approbation de l'accord-cadre de Waterfront Toronto et les incohérences relatives aux témoignages de ses représentants devant le Comité ont miné la confiance des néo-démocrates à l'égard de ce projet.

Capitalisme de surveillance et démocratie

Le capitalisme de surveillance et le modèle d'affaires de Sidewalk Labs Le Comité a récemment entendu de nombreux témoignages d'éminents spécialistes sur ce que l'on appelle de plus en plus le « capitalisme de surveillance ». Il a notamment été question des risques qu'il représente pour les droits démocratiques des citoyens, tant par son modèle d'affaires, qui constitue fondamentalement un affront à l'autonomie humaine, que par le pouvoir institutionnel et commercial qu'il procure aux entreprises qui le pratiquent, comme Alphabet, Facebook et Amazon.

M[me] Shoshana Zuboff, Ph. D., professeure émérite à la Harvard Business School et auteure de l'ouvrage *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power,* a expliqué au Comité que le capitalisme de surveillance est « une vaste logique économique systémique qui, à notre connaissance, est sans précédent », en ce sens qu'il « se saisit de l'expérience humaine privée et il la subordonne aux dynamiques de marché[15] ».

---

[11] Di Lorenzo, mémoire, p. 2.
[12] *Ibid*., p. 3.
[13] *Ibid*., p. 3.
[14] Vérificatrice générale, Société de revitalisation du secteur riverain de Toronto, p. 806.
[15] Shoshana Zuboff, témoignage devant le Comité permanent de l'accès à l'information, de la protection des renseignements personnels et de l'éthique, 27 mai 2019.

M[me] Zuboff affirme que, tout comme les incarnations précédentes du capitalisme, « il prend quelque chose qui existe à l'extérieur du marché et il le transforme en marchandise pouvant être produite et vendue. Comme chacun le sait, le capitalisme industriel s'est emparé de la nature et il l'a convertie en terres ou en propriétés foncières pouvant être vendues ou achetées ». Selon elle, le capitalisme de surveillance « se saisit de l'expérience humaine privée et il la subordonne aux dynamiques de marché[16] ».

M[me] Zuboff a ajouté que le capitalisme de surveillance transforme l'expérience humaine privée « en matière première gratuite, qui est ensuite convertie en données comportementales. Certes, une partie des données comportementales sont utilisées pour améliorer les produits et les services, mais le reste forme un excédent comportemental, qui est reconnu pour sa grande valeur de prédiction ».

Cet « excédent comportemental » devient, par l'application des technologies d'apprentissage machine, un « produit prédictif » : « On les vend dans une nouvelle sorte de marché qui fait uniquement le commerce d'avenirs humains. Le premier marché de cette sorte était celui de la publicité ciblée en ligne. Les prédictions humaines qui y étaient vendues s'appelaient les taux de clics. Vous n'avez qu'à prendre un pas de recul pour comprendre que le taux de clics n'est qu'un fragment d'une prédiction d'un avenir humain ».

Celles-ci sont ultimement utilisées par les plates-formes capables d'exploiter les économies d'envergure et les économies d'échelle pour offrir à leurs clients des services perfectionnés permettant de prédire et même de déterminer les comportements des utilisateurs (autrement dit, de modifier leurs habitudes)[17].

En fin de compte, a fait valoir M[me] Zuboff, l'objectif du modèle consiste à ce que « l'analyse informatique du capitalisme de surveillance qui favorise ses propres résultats commerciaux remplace la démocratie et la gouvernance telles que nous les connaissons[18] ». M. Roger McNamee, investisseur aguerri de la Silicon Valley et l'un des premiers à avoir investi dans Facebook, a corroboré ces propos en disant que, pour les adeptes du capitalisme de surveillance, « la manipulation comportementale est le but[19] ».

M[me] Zuboff a déclaré que, pour faire échec aux torts causés par le capitalisme de surveillance, les législateurs et les organismes de réglementation doivent concevoir « des stratégies qui interrompent et, dans bien des cas, rendent illégaux les mécanismes fondamentaux du capitalisme de surveillance. Il s'agit notamment de l'appropriation unilatérale de l'expérience humaine privée en tant que source gratuite de matières brutes et sa transformation en données. Ces mécanismes comprennent également les asymétries extrêmes sur le plan de l'information qui sont nécessaires pour prédire le comportement humain. Ils comprennent également la fabrication de produits de prédiction informatique fondés sur la consignation unilatérale et secrète de l'expérience humaine[20] ».

À propos des villes intelligentes, M[me] Zuboff a déclaré ceci : « La visée est la ville intelligente. Si le capitalisme de surveillance peut conquérir la ville intelligente, il peut conquérir aussi la société

[16] Zuboff, témoignage, 27 mai 2019.
[17] Shoshana Zuboff, témoignage devant le Comité permanent de l'accès à l'information, de la protection des renseignements personnels et de l'éthique, 28 mai 2019.
[18] Shoshana Zuboff , témoignage, 28 mai 2019.
[19] Roger McNamee, témoignage devant le Comité permanent de l'accès à l'information, de la protection des renseignements personnels et de l'éthique, 28 mai 2019.
[20] Shoshana Zuboff , témoignage, 28 mai 2019.

démocratique. Aujourd'hui, le combat se livre à Toronto. Si le Canada donne Toronto à Google, ou plutôt à Alphabet — Sidewalk Labs maintient maintenant avidement qu'elle ne fait pas partie de Google —, l'avenir de la société démocratique au XXIe siècle sera menacé ». Dans son témoignage, Mme Zuboff a dit expressément que Sidewalk Toronto représente « une réincarnation d'un genre de tyrannie absolutiste que nous pensions avoir laissée derrière nous au XVIIIe siècle, mais qui est maintenant servie avec un cappuccino et enrobée de uns et de zéros ». Selon elle, « c'est une façon directe pour l'entreprise de contourner la démocratie afin d'imposer sa vision, qui, au bout du compte, vise ses propres objectifs commerciaux précis[21] ».

M. Jim Balsillie, fondateur et ancien chef de la direction de Research in Motion, a aussi déclaré ceci devant le comité: « La technologie perturbe la gouvernance; si on ne la contrôle pas, elle pourrait entraîner l'obsolescence de la démocratie libérale […] La technologie est en train de devenir le nouveau quatrième pouvoir. Dans notre système de freins et contrepoids, la technologie est ainsi mise sur un pied d'égalité avec l'exécutif, le législatif et le judiciaire ». M. Balsillie a précisé ses dires en déclarant ceci : « nous, les Canadiens, menons actuellement une bataille historique pour l'avenir de notre démocratie contre une mascarade appelée Sidewalk Toronto[22] ».

M. McNamee, parlant expressément de Sidewalk Toronto, a déclaré ceci : « Je ne laisserais pas Google venir à moins de 100 miles de Toronto. Le problème fondamental ici, c'est l'autonomie gouvernementale et l'autodétermination. Je crois qu'aucune entreprise — pas Google ni qui que ce soit — ne devrait être responsable de gérer nos espaces publics et nos infrastructures municipales. Il y a une limite à ce qu'on peut faire avec un partenariat public-privé, et cela va bien au-delà de cette limite. »

Il a ajouté ceci: « [J]e demeure prudent par rapport à la question de la collecte de données. Je crois que les problèmes sous-jacents à la surveillance créent trop de tentations pour les gens. À l'heure actuelle, il est beaucoup trop difficile de surveiller ce que font ces entreprises avec les données après les avoir recueillies. À mon sens, comme on dit souvent au gouvernement, il faut étudier encore davantage tous ces aspects avant d'aller de l'avant[23]. »

Les néo-démocrates croient que le capitalisme de surveillance, en tant que modèle commercial, présente un grave risque pour le gouvernement démocratique et l'autonomie humaine. En outre, ils prennent au sérieux les préoccupations soulevées par Mme Zuboff, M. McNamee et M. Balsillie au sujet de l'incertitude et des risques inhérents au projet Sidewalk Toronto, et ils croient que les Torontois sont tout à fait en droit d'exiger davantage pour eux-mêmes et leur collectivité.

La notion de « ville intelligente » promet des services et des commodités qui n'ont rien de néfaste en soi; les néo-démocrates estiment qu'un tel projet peut s'avérer très prometteur, pourvu qu'il soit mené de façon responsable et selon les principes de la démocratie.

Cependant, compte tenu du modèle d'affaires axé sur le capitalisme de surveillance que propose Alphabet, société mère de Sidewalk, et des préoccupations exprimées ci-dessus à ce sujet, les néo-démocrates n'ont d'autre choix que de conclure que le gouvernement du Canada, le gouvernement de

[21] *Ibid*.
[22] Jim Balsillie, témoignage devant le Comité permanent de l'accès à l'information, de la protection des renseignements personnels et de l'éthique, 28 mai 2019.
[23] Roger McNamee, témoignage, 28 mai 2019.

l’Ontario et la Ville de Toronto devraient aborder ce projet avec beaucoup scepticisme et se montrer très prudents avant de prendre des engagements à long terme au nom des citoyens.