CHAMBRE DES COMMUNES
HOUSE OF COMMONS
CANADA

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

ETHI • NUMÉRO 096 • 1re SESSION • 42e LÉGISLATURE

TÉMOIGNAGES

Le jeudi 22 mars 2018

Président

M. Bob Zimmer

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

Le jeudi 22 mars 2018

● (0850)

[*Traduction*]

Le président (M. Bob Zimmer (Prince George—Peace River—Northern Rockies, PCC)): Je déclare la 96e réunion du Comité permanent de l'accès à l'information, de la protection des renseignements personnels et de l'éthique ouverte. Conformément au sous-alinéa 108(3)h)(vii) du Règlement, nous étudions la protection des données personnelles dans les services gouvernementaux numériques, une étude de la e-Governance Academy. Nous accueillons, par téléconférence, Liia Hänni, experte principale, et Raul Rikk.

Nous venons tout juste d'être informés que les témoins ont une présentation, mais elle est uniquement en anglais. Ils ne l'ont pas fait traduire en français, alors je vais demander le consentement unanime afin qu'ils puissent présenter leur exposé au Comité maintenant. Y a-t-il consentement unanime?

Des députés: D'accord.

Le président: Merci. Nous pouvons maintenant passer à la déclaration en anglais seulement.

Allez-y. Raul, vous nous entendez?

Allez-y, monsieur Erskine-Smith.

M. Nathaniel Erskine-Smith (Beaches—East York, Lib.): Puisque nous avons un peu de temps, M. Angus a donné avis d'une motion liée à l'enjeu qu'on a pu lire dans les nouvelles au sujet de Christopher Wylie et de Facebook. Notre travail consiste à protéger du mieux que nous pouvons les renseignements personnels des Canadiens, et, par conséquent, je veux obtenir le consentement unanime afin que nous adoptions cette motion aujourd'hui.

Le président: Est-ce que tous les membres ont vu la motion?

M. Nathaniel Erskine-Smith: Si on ne peut pas adopter officiellement la motion de M. Angus, alors je propose un libellé identique.

Des députés: Ah, ah!

M. Nathaniel Erskine-Smith: Lorsqu'on obtient le consentement des analystes, on peut tout faire.

Le président: Je parlais justement à Jean-Denis, et ce dont nous avons besoin, c'est un consentement unanime pour adopter la motion. Avons-nous un consentement unanime quant à l'adoption de la motion?

Des députés: D'accord.

Le président: Monsieur Erskine-Smith, voulez-vous présenter votre motion?

M. Nathaniel Erskine-Smith: Je propose, et je reprends ainsi le libellé de la motion de M. Angus, que nous invitions Christopher Wylie, des représentants de Facebook, et d'autres intervenants, y compris le commissaire à la protection de la vie privée pour discuter des récentes répercussions sur la vie privée pour le Canada et les Canadiens relativement à la récente attention médiatique portée sur Cambridge Analytica.

Le président: Peut-on dire sans se tromper que c'est exactement le libellé de la motion de M. Angus?

M. Nathaniel Erskine-Smith: La motion est identique à celle de M. Angus.

Le président: Allez-y.

[*Français*]

Mme Anne Minh-Thu Quach (Salaberry—Suroît, NPD): J'ai le texte, ici. Je ne sais pas si vous voulez que je le lise.

[*Traduction*]

M. Nathaniel Erskine-Smith: Oui, je l'ai, ici.

[*Français*]

Mme Anne Minh-Thu Quach: Je peux le lire, si vous le voulez. Je vais le lire en français, évidemment:

> Que, compte tenu de la vaste atteinte à la protection des données commise par Cambridge Analytica et de son non-signalement par Facebook pendant plusieurs années, le Comité étudie les répercussions sur la vie privée des monopoles de plateforme ainsi que les solutions législatives et réglementaires nationales et internationales possibles pour assurer la confidentialité des données des citoyens et l'intégrité des processus démocratiques et électoraux dans le monde, et qu'il entende...

[*Traduction*]

Le président: Il n'y a pas de traduction fournie, alors je me demande si c'est...

[*Français*]

Mme Anne Minh-Thu Quach: Dois-je recommencer? A-t-on la traduction, maintenant?

C'est important que la traduction fonctionne, et pas seulement dans un sens.

[*Traduction*]

M. Nathaniel Erskine-Smith: Nous avons une motion par écrit, cependant, de M. Angus, et nous avons obtenu le consentement unanime pour l'adopter. Nous adoptons simplement la motion de M. Angus, dont l'avis a déjà été reçu. Franchement, je ne crois même pas qu'il soit nécessaire de la lire.

Le président: Pour que ce soit clair, est-ce que la motion de M. Angus est une motion du NPD?

[*Français*]

Mme Anne Minh-Thu Quach: Oui.

[*Traduction*]

Le président: Vous avez présenté la motion. Quelqu'un veut-il en discuter? Nous allons mettre la motion aux voix.

(La motion est adoptée. [*Voir le Procès-verbal*])

Le président: Merci, monsieur Erskine-Smith. Allez-y.

M. Nathaniel Erskine-Smith: Puisque nous accueillons nos témoins, aujourd'hui, puis, M. Fishenden, mardi, et l'ancien président de l'Estonie, jeudi, et que nous allons ensuite terminer l'étude sur la neutralité d'Internet, je suggère au Sous-comité de se réunir mardi durant la deuxième heure, après le témoignage de M. Fishenden, pour déterminer les témoins à rencontrer dans le cadre de cette étude.

Le président: D'accord. Oui, je suis sûr que nous pouvons...

Allez-y.

[*Français*]

Mme Anne Minh-Thu Quach: Je m'excuse, mais y a-t-il moyen d'avoir les textes des présentations maintenant? Habituellement, par principe, nous sommes censés recevoir toutes les présentations dans les deux langues officielles.

[*Traduction*]

Le président: Vous parlez de la présentation, ici?

[*Français*]

Mme Anne Minh-Thu Quach: Habituellement, pour toutes les présentations dans tous les comités, s'il n'y a pas...

[*Traduction*]

Le président: Nous venons d'adopter une motion visant à accepter à l'unanimité la présentation de l'exposé en anglais seulement, nous avons déjà mis cette question aux voix.

[*Français*]

Mme Anne Minh-Thu Quach: C'est simplement que je pensais que nous aurions la présentation en anglais, mais avec les textes. Toutefois, les textes vont nous arriver seulement plus tard. Par principe, je m'oppose à cela, habituellement. Nous sommes dans une institution bilingue. Je suis désolée, mais...

[*Traduction*]

Le président: À ce que je sache, il n'y a pas là d'enjeu lié au bilinguisme. Nous avons déjà accepté à l'unanimité que la présentation soit faite en anglais seulement. Le Comité vient de l'accepter à l'unanimité. Je ne sais pas exactement quel est le problème, ici.

À part voir la présentation physiquement, devant vous, vous la verrez à l'écran, directement devant vous, durant l'exposé.

Allez-y, monsieur Picard.

[*Français*]

M. Michel Picard (Montarville, Lib.): J'ai deux points à soulever.

Certains défendent la place de la langue française, et j'en fais certainement partie. Cela dit, il y a deux choses. Premièrement, il faut tenir compte de la réalité à laquelle nous sommes exposés et nous montrer flexibles. Je pense que la situation d'aujourd'hui est exceptionnelle. Deuxièmement, le consentement unanime a été obtenu conformément à la procédure. Je pense donc que le débat n'a pas lieu d'être.

[*Traduction*]

Le président: D'accord. Les documents seront traduits.

Liia Hänni et Raul Rikk, vous pouvez présenter votre déclaration. Allez-y, s'il vous plaît.

Nos techniciens viennent de dire que votre appareil est en mode sourdine actuellement. Pouvez-vous activer le micro de votre appareil, s'il vous plaît?

● (0855)

M. Nathaniel Erskine-Smith: Je ne sais pas si c'est de bon augure pour une étude sur le gouvernement numérique.

Des voix: Ah, ah!

Le président: Je crois que nous avons maintenant du son.

Veuillez nous présenter votre exposé.

Mme Liia Hänni (experte principale, e-Governance Academy): D'accord.

Pour commencer, c'est vraiment une excellente tribune, et nous apprécions de pouvoir participer à cette réunion virtuelle avec vous. Je m'appelle Liia Hänni. Je suis experte principale de la démocratie numérique et de la gouvernance ouverte, et je suis très heureuse de vous communiquer certains de nos points de vue sur la façon dont les renseignements personnels peuvent être protégés dans des systèmes de gouvernement numérique. Je crois savoir que c'est là votre principale préoccupation au Canada, l'élaboration de systèmes gouvernementaux numériques sécuritaires pour votre pays.

Vous savez peut-être que, en Estonie, nous avons réussi à créer un système de gouvernement numérique qui est beaucoup utilisé par les citoyens estoniens. Selon moi, nous devons, dans un premier temps, vous expliquer les fondements du gouvernement numérique sécuritaire en Estonie. J'ai eu l'occasion hier de présenter un exposé à une délégation canadienne de membres de votre Secrétariat du Conseil du Trésor, alors je comprends maintenant les genres d'enjeux auxquels vous êtes confrontés au Canada.

En Estonie, le gouvernement numérique...

[*Français*]

Mme Anne Minh-Thu Quach: Je ne reçois pas l'interprétation.

[*Traduction*]

Mme Liia Hänni: Est-ce que vous m'entendez?

Le président: Je suis désolé. Je dois vous demander d'arrêter une seconde.

Allez-y, madame Quach.

[*Français*]

Mme Anne Minh-Thu Quach: Je ne reçois pas l'interprétation. Je ne sais pas si d'autres l'obtiennent, mais je n'ai aucune interprétation pour le moment.

[*Traduction*]

Le président: Je suis désolé, tout le monde. Nous devons suspendre la réunion pendant deux minutes.

Madame Hänni, veuillez s'il vous plaît patienter deux minutes pendant que nous réglons tout ça. Je suis désolé.

● (Pause)

●

● (0900)

Le président: Nous allons reprendre nos travaux. Les interprètes ne pouvaient pas faire leur travail en raison d'un écho dans le dispositif.

Encore une fois, toutes mes excuses à Liia et Raul. Veuillez poursuivre. Tout devrait bien aller maintenant.

M. Raul Rikk (directeur de programme, Cybersécurité nationale, e-Governance Academy): Je vous souhaite moi aussi le bonjour.

Je m'appelle Raul Rikk. Je travaille pour la e-Governance Academy en tant que directeur de programme de la cybersécurité nationale.

J'ai acquis mon expérience dans le secteur de la sécurité en Estonie. Il y a des années de cela, j'ai été responsable de l'établissement du Centre d'excellence de l'OTAN pour la cyberdéfense en coopération, à Tallinn. J'ai travaillé dans le domaine de la cybersécurité et de la protection des données pendant 15 ans.

Merci de nous avoir invités à présenter le modèle estonien en matière de protection des données dans une société numérique et de cybersécurité. Puisque nous procédons par vidéoconférence, nous avons décidé de ne pas passer toute la présentation en revue. Nous allons tout simplement utiliser une diapositive qui réunit tous les différents aspects dont nous discuterons probablement aujourd'hui. Cette diapositive souligne les principaux principes dans le domaine de la protection des données de la cybersécurité et décrit l'architecture générale garantissant l'interopérabilité et la sécurité dans l'environnement numérique estonien.

Selon moi, nous pouvons aller directement aux questions. Il est probablement préférable de procéder de cette façon.

Le président: C'est ce que nous ferons, alors. Merci.

Je tiens à dire aux membres du Comité qu'il y a un délai d'environ trois secondes avant qu'ils nous entendent, même si on n'en est pas conscient.

Nous allons commencer par Mme Vandenbeld, pour sept minutes.

Mme Anita Vandenbeld (Ottawa-Ouest—Nepean, Lib.): Merci beaucoup, monsieur le président.

Pour commencer, je tiens à saluer Liia, avec qui j'ai travaillé dans le passé. J'admire vraiment votre travail.

Merci à vous deux d'être là et de comparaître devant le Comité ce matin.

J'aimerais demander à Liia de quelle façon tout ça a commencé en Estonie. Nous savons que l'Estonie est l'un des pays à l'avant-garde lorsqu'il est question de gouvernance électronique. Quand l'idée a-t-elle vu le jour? Qu'est-ce qui était à la base? Par où avez-vous commencé pour vous rendre où vous êtes rendus maintenant?

● (0905)

Mme Liia Hänni: Merci.

Bien sûr, c'est une longue histoire, parce que l'Estonie vient de célébrer ses 100 ans, et que nous sommes à nouveau indépendants depuis 27 ans.

Nous avons eu cette occasion de tout recommencer à neuf, en commençant par une nouvelle constitution. Immédiatement, nous nous sommes demandé de quelle façon nous pouvions respecter toutes les exigences démocratiques en partant de la situation... nous avons décidé qu'il fallait utiliser le pouvoir de la technologie.

C'était une décision importante. De plus, nous constations que les politiques sont importantes. Si on dote un pays et une société d'une vision stratégique, on peut faire beaucoup de choses. Une bonne partie de ces genres de principes stratégiques étaient vraiment nouveaux, mais on les a adoptés pour le bien-être de tous les membres de la société. Personne n'a été laissé pour compte lorsque nous avons mis au point le gouvernement numérique et notre société de l'information.

De plus, notre conviction, c'était qu'une structure et un modèle de gouvernance numérique en Estonie devaient être une plateforme pour toute la société, pas seulement pour le gouvernement. C'est un avantage que nous tirons de la gouvernance numérique. Le système doit être destiné à tous les citoyens de l'Estonie. À la lumière de ces principes, nous avons créé le modèle qui figure sur la diapositive de Raul.

Le modèle estonien compte trois composantes importantes. Premièrement, notre gouvernement nous donne une forte identité numérique. Notre vision, c'est que c'est le rôle du gouvernement non seulement de délivrer des passeports papier, mais aussi des certificats numériques et des outils d'identification numérique pour les citoyens. C'est l'un des fondements du système de gouvernance numérique estonien.

La deuxième composante, ce sont les données et ressources numériques. Nous avons des centaines de bases de données pouvant accueillir des données numériques, mais ce n'est pas suffisant d'avoir de bons services électroniques pour nos citoyens. Il faut assurer l'interopérabilité. Cela signifie que ces nombreux ensembles de données doivent être contenus dans un système uniforme. C'est ce qu'on a réalisé en Estonie grâce à un système que nous appelons X-Road, qui nous a permis de connecter tous les ensembles de données dans un seul système. C'est là l'architecture de base du gouvernement numérique estonien.

Troisièmement, le gouvernement numérique n'est pas constitué d'ensembles de données distincts. C'est un système qui doit être doté d'une architecture bien établie. Beaucoup de personnes considèrent ce qui précède comme des composantes de base du modèle de gouvernement numérique en Estonie. Le système X-Road permet la tenue des données numériques sur les citoyens et l'interopérabilité à l'échelle du système.

Mme Anita Vandenbeld: Je constate que vous faites un lien direct entre la démocratie et la gouvernance numérique ou gouvernance électronique, ce qui, selon moi, est très intéressant.

Je sais que votre institut a travaillé auprès de 90 pays du monde entier. Pouvez-vous nous parler rapidement de certains des défis auxquels différents pays sont confrontés et de certaines des leçons apprises, particulièrement lorsqu'on tient compte du fait que l'Estonie est un très petit pays? Le Canada, bien sûr, est un grand pays possédant un grand territoire. Voyez-vous des différences dans l'application des leçons apprises en Estonie lorsque vous vous rendez dans différents pays du globe?

Mme Liia Hänni: Je crois que la taille d'un pays n'est pas aussi importante qu'elle peut le sembler à première vue. Les défis que nous rencontrons sont toujours les mêmes. Tous les gouvernements veulent avoir un bon système de gouvernance numérique et fournir de bons services numériques à leurs citoyens, mais, pour ce faire, il y a certaines conditions préalables. J'en ai mentionné trois. Habituellement, ce qui manque dans différents pays, c'est la compréhension qu'un gouvernement numérique ne doit pas être composé de systèmes d'information distincts, et que tous ces systèmes doivent travailler ensemble.

C'est principalement une question d'interopérabilité, qui est non seulement un enjeu technique, mais, dans un premier temps, un enjeu organisationnel. Différents organismes étatiques devraient pouvoir travailler en collaboration et partager des données et offrir les services électroniques que nous offrons en Estonie.

● (0910)

M. Raul Rikk: Si je peux me permettre d'ajouter quelque chose, la situation qu'on constate habituellement dans différents pays, c'est que des organisations distinctes ont mis en place leur propre système, et ces systèmes ne fonctionnent pas ensemble. C'est le problème vraiment fondamental.

Le deuxième problème, c'est la façon d'assurer la sécurité si on crée une connexion entre les différents systèmes. C'est la situation typique rencontrée dans différents pays. C'est exactement ce avec quoi nous devons composer chaque jour.

Mme Liia Hänni: Je tiens tout de même à souligner à quel point l'identité numérique est importante, parce que sans un tel système solide d'identité numérique, les gens ne peuvent pas utiliser leurs propres services publics protégés. C'est leur carte d'identité, celle qu'ils utilisent déjà depuis 15 ans. C'est un élément vraiment fondamental du système économique sécurisé d'Estonie. Raul, bien sûr, peut expliquer de quelle façon cela protège aussi les données dans le système estonien.

Le président: Merci, madame Vandenbeld. Le temps est écoulé.

Nous passons à M. Kent pour sept minutes.

L'hon. Peter Kent (Thornhill, PCC): Merci beaucoup, monsieur le président, et merci à vous deux de votre patience tandis que nous tentions de surmonter certains défis techniques. J'ai encore de la difficulté à entendre tout ce que vous dites, avec tous les messages, mais nous allons poursuivre. C'est peut-être plus là le reflet de mon âge que des limites techniques du système.

Monsieur Rikk, il y a un certain nombre d'années, durant une étude parlementaire sur la défense de l'Amérique du Nord, une personne faisant autorité dans le domaine cybernétique nous a dit que toutes les défenses et les applications de sécurité étaient, au mieux, temporaires, parce qu'Internet était conçu en fonction d'un principe d'ouverture, une notion d'ouverture, ce qui fait en sorte que, tôt ou tard, les meilleures mesures de sécurité peuvent toujours être contournées.

Puisque vous êtes voisin d'un des pays qui s'adonnent le plus au cybervandalisme dans le monde actuellement, quelles sont l'intensité et la fréquence de vos vérifications de la sécurité de votre système?

M. Raul Rikk: Je peux vous assurer que la situation est exactement celle mentionnée dans le rapport... [*Difficultés techniques*].

Le président: Attendez, Raul, il n'y a plus de son du tout.

Raul, est-ce que votre micro est près de vous lorsque vous parlez, ou est-il plus loin? Si vous pouvez rapprocher le micro, cela nous aiderait beaucoup.

M. Raul Rikk: Le micro est de l'autre côté de la table, mais le fil n'était pas...

Le président: Si vous pouvez le rapprocher, cela nous aiderait beaucoup, parce qu'il y a beaucoup d'écho. C'est très difficile d'entendre ce que vous dites.

M. Raul Rikk: Vous m'entendez, maintenant?

Le fil est... je devrai m'asseoir plus près, alors.

Le président: Si c'est possible, nous serions reconnaissants. Nos interprètes ont beaucoup de difficulté à vous suivre.

M. Raul Rikk: Vous pouvez peut-être tourner la caméra afin que vous puissiez mieux nous voir. Nous sommes maintenant à côté du microphone.

Est-ce que c'est bien? Est-ce que je poursuis?

● (0915)

Le président: D'accord. Raul, si vous parlez, alors on voit que c'est mieux.

M. Raul Rikk: Je confirmerai que l'étude dont vous avez parlé est correcte. Notre approche en matière de cybersécurité, c'est qu'il s'agit d'un processus continu. Nous travaillons quotidiennement pour l'améliorer sans cesse et assurer la coordination avec le développement général des TIC.

Voici seulement un exemple. Tout le système de sécurité que nous utilisons en Estonie est fondé sur un système de chiffrement à la fine pointe de la technologie. Le chiffrement, c'est une technologie qu'il faut mettre à niveau au moins tous les deux ou trois ans. Nous avons un service spécial qui s'occupe de ça. Les responsables réalisent des études sur le chiffrement et soutiennent la mise en oeuvre des nouveaux systèmes de chiffrement tous les deux ou trois ans.

L'hon. Peter Kent: Si je peux poursuivre, alors, quel appareil les citoyens utilisent-ils pour avoir accès aux services? Avez-vous une clé de chiffrement associée à un mot de passe qui change régulièrement? De quelle façon procédez-vous?

M. Raul Rikk: C'est exactement ce dont Liia Hänni parlait au sujet des cartes d'identité que nous utilisons. Nous les appelons des cartes d'identité, mais du point de vue de la sécurité, c'est un appareil de chiffrement que possède chaque citoyen estonien. Sur les cartes d'identité, il y a une puce qui contient un cryptoprocesseur. Alors, essentiellement, lorsqu'un citoyen utilise une carte d'identité, il utilise en fait un système de chiffrement.

L'hon. Peter Kent: Ma prochaine question concerne l'un des points que vous avez soulevés, un des principes de base de la cybersécurité selon lequel il ne doit pas y avoir de chevauchement entre les bases de données. Avez-vous centralisé les bases de données des différents services que vous offrez sur ce système central? Avez-vous eu des problèmes liés au fait que diverses institutions hésitaient à céder leur pouvoir?

M. Raul Rikk: 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.

Mme Liia Hänni: C'est le principe « une fois pour toutes » appliqué en Estonie: le gouvernement ne peut pas me demander des données si je les ai déjà fournies dans un autre système d'information estonien.

L'hon. Peter Kent: Merci, monsieur le président.

Le président: Merci, monsieur Kent. Encore une fois, toutes mes excuses pour la situation. Tout était censé être réglé avant, mais il semble que nous vous entendons maintenant et que les choses vont mieux.

Nous passons maintenant à Mme Quach.

[*Français*]

Mme Anne Minh-Thu Quach: Merci, monsieur le président.

Je remercie les deux invités de l'Estonie.

Je voulais savoir quels types de mécanismes de surveillance et de protection des données le gouvernement du Canada doit déployer pour éviter les brèches de sécurité et les attaques numériques. Je pense à cette affaire d'échange de données personnelles dans le cas de Facebook, dont on entend beaucoup parler dans l'actualité. Faut-il agir du côté des lois? Quels types de ressources, qu'il s'agisse d'argent ou d'expertise, doit-on déployer pour assurer cette protection?

● (0920)

[*Traduction*]

M. Raul Rikk: Il n'y a pas une seule réponse, ici, parce que lorsque nous parlons de sécurité, il y a trois catégories principales qu'il faut garder à l'esprit.

Premièrement, c'est la confidentialité. Les atteintes peuvent viser la confidentialité.

Deuxièmement, il y a l'intégrité des données. Cela signifie, par exemple, que, dans le registre de la population où sont conservés les noms des citoyens, il n'y a rien de secret au sujet des noms, mais il faut assurer l'intégrité de ces données. Nous devons les protéger afin que personne ne puisse avoir accès au registre des populations afin de modifier mon nom, par exemple.

Troisièmement, c'est l'accessibilité de l'information. Cela signifie qu'il faut protéger le réseau et la communication des données afin que tout le monde puisse avoir accès aux données lorsqu'il en a besoin. On tient toujours compte de ces trois aspects lorsqu'il est question de cybersécurité.

Selon moi, lorsque cela concerne, par exemple, Facebook, alors on ne peut rien faire du point de vue de l'accessibilité. Votre question portait sur la protection des données personnelles, et, dans ce cas, seule la réglementation peut servir parce qu'elle transfère la responsabilité à l'entreprise qui fournit le service. C'est là exactement pourquoi l'Union européenne a adopté le nouveau Règlement général sur la protection des données qui donne le pouvoir sur les données aux propriétaires des données, les citoyens, tout en imposant un meilleur contrôle des entreprises fournissant les services numériques.

[*Français*]

Mme Anne Minh-Thu Quach: Une partie de votre explication m'a échappé. J'ai seulement compris, à la fin, que c'étaient les citoyens qui avaient le contrôle de leur sécurité. Toutefois, comment le gouvernement peut-il s'assurer, en cas de brèche, qu'il y a une divulgation ou même des sanctions? Je ne sais pas si des sanctions sont prévues, en Estonie.

Quelle autorité s'assure qu'il y a une protection des données et voit à ce qu'on rectifie le tir, en cas de brèche? Si ce sont les citoyens qui doivent le faire, ils ne sont pas nécessairement outillés pour détecter une violation des droits à la vie privée. Qui assure cette surveillance dans le cas des services gouvernementaux?

[*Traduction*]

M. Raul Rikk: C'est l'objectif, justement, du Règlement général sur la protection des données, de mettre en place différents mécanismes pour contrôler les fournisseurs de services numériques. Un principe très similaire, c'est que, par exemple, en tant que propriétaire de données, je dois toujours avoir une idée de la façon dont mes données sont utilisées. Par exemple, si j'utilise Facebook, lorsque j'approche Facebook et que je veux savoir de quelle façon l'entreprise utilisera mes données, cette dernière doit me donner un aperçu total de la façon dont ça se fait. De plus, si je veux effacer certaines données, l'entreprise doit le faire. En outre, le troisième principe, c'est que les entreprises ne peuvent pas prendre des engagements à long terme. Par exemple, si une entreprise me demande si je suis prêt à céder le pouvoir à l'égard de mes données pendant 10 ans, elle ne peut pas le faire légalement. Le jour suivant, je peux communiquer avec l'entreprise pour dire que je ne veux plus qu'elle utilise mes données, et elle doit les effacer. Il y a plusieurs mécanismes de réglementation pour contrôler tout ça.

De plus, si quelque chose se produit, il y a de très importantes sanctions contre les entreprises, jusqu'à 4 % du chiffre d'affaires global. Cette réglementation entraîne d'importants changements, du moins en Europe, au sein des entreprises qui fournissent des services numériques.

● (0925)

[*Français*]

Mme Anne Minh-Thu Quach: Quelle autorité effectue la surveillance? Est-ce votre commissaire en matière de protection de la vie privée et d'éthique qui veille à ce que toutes ces lois soient respectées et à ce que les compagnies privées qui offrent les services soient surveillées? Est-ce fait par cette autorité?

[*Traduction*]

M. Raul Rikk: En Estonie, nous avons un organisme de protection des données, et chaque pays européen qui appartient à l'Union européenne doit se doter d'un tel organisme. L'organisme a le pouvoir de superviser tout ce qui est lié à la protection des données.

[*Français*]

Mme Anne Minh-Thu Quach: C'est parfait.

[*Traduction*]

M. Raul Rikk: En fait, c'est un domaine auquel l'Union européenne s'est beaucoup intéressée au cours des 10 à 15 dernières années.

[*Français*]

Mme Anne Minh-Thu Quach: D'accord.

Quelle est l'ampleur des investissements gouvernementaux?

[*Traduction*]

M. Raul Rikk: Je n'ai pas les chiffres, mais en ce qui concerne les dossiers estoniens, l'agence compte environ 100 personnes. Ce n'est pas une grosse organisation, mais je dirais que, au fil des ans, son rôle est devenu plus important, parce que toute la société est maintenant numérisée.

Le président: Merci, madame Quach.

Nous allons maintenant passer à M. Erskine-Smith, pour sept minutes.

M. Nathaniel Erskine-Smith: Merci beaucoup.

Précédemment, lorsque le Comité a réalisé une étude sur l'échange d'information, des témoins ont laissé entendre qu'une loi mise en place par l'administration précédente était trop permissive en ce qui concerne la communication des renseignements. Puisque vous utilisez le principe « une fois pour toutes » et que des organismes estoniens peuvent avoir accès, à l'aide du système d'échange de données sécurisées, plus facilement aux renseignements personnels, de quelle façon dissipez-vous les préoccupations possiblement trop permissives de l'information?

M. Raul Rikk: Dans notre cas, en fait, pas un seul organisme ne peut avoir accès à tous les renseignements échangés. C'est la raison pour laquelle ce que vous voyez, sur la diapositive, c'est chaque voie. Cet environnement d'échange de données sécurisé, c'est aussi ce que nous appelons l'Internet sécurisé. Il fonctionne de la même façon qu'Internet. L'échange de données se passe entre différentes organisations ou entre des organisations et des citoyens. Tous ces processus d'échange d'information sont chiffrés et bloqués et personne d'autre ne peut y accéder. Il n'y a pas un seul organisme qui peut avoir le contenu des renseignements échangés.

Dans le cas d'un organisme chargé de la sécurité ou d'une enquête policière, les intervenants doivent avoir un code, une permission, pour mener l'enquête. Cela se produit conformément à la réglementation sur les enquêtes. En principe, les gens peuvent seulement voir les données pour lesquelles ils ont une autorisation. C'est la raison pour laquelle vous voyez les voies sur la diapositive. Premièrement, on peut entrer dans le système en tant que citoyen ou représentant du gouvernement ou encore membre du milieu des affaires. Dans chaque cas, la présentation est différente. Cela dépend aussi de votre rôle personnel. Vous pouvez seulement voir les ensembles de données que vous êtes autorisé à voir.

M. Nathaniel Erskine-Smith: Merci.

Je sais que nous avons des préoccupations, ici, au Canada, parfois, au sujet du vol d'identité. L'exemple classique actuellement et depuis un certain nombre d'années, ce sont les fraudeurs qui appellent des gens, particulièrement des aînés, mais aussi d'autres personnes, en se faisant passer pour notre agence du revenu.

Vos citoyens ont une carte d'identité permettant éventuellement d'avoir accès à tous les services gouvernementaux. Je comprends que vous avez dit qu'il y a un chiffrement et que la carte est, en fait, chiffrée, mais de quelle façon l'Estonie compose-t-elle avec le possible vol d'identité grâce à ces cartes? Est-ce que cela est une préoccupation? Quels sont les processus mis en place pour composer avec cette situation?

● (0930)

M. Raul Rikk: Cela peut être surprenant, mais, depuis que nous avons mis en oeuvre le système des cartes d'identité électroniques, nous n'avons pas eu de cas de vol d'identité. Nous avons eu des cas liés à des activités sur Facebook, mais ce n'est pas la même chose. En ce qui concerne les cartes d'identité et l'accès et l'utilisation des services gouvernementaux, nous n'avons pas eu de cas de vol d'identité. C'est en raison de la carte d'identité.

Pour être plus précis, la carte d'identité n'est pas chiffrée, mais la carte d'identité en tant que telle est un appareil de chiffrement. En utilisant ma carte d'identité, je peux créer une connexion sécurisée avec les services gouvernementaux, ou aussi avec des services privés, par exemple, les services bancaires.

La carte d'identité est délivrée par le gouvernement de la même façon que le sont les passeports. Elle est électronique et conçue spécialement pour le cyberespace. Grâce à ce processus gouvernemental d'identification des personnes et de délivrance des cartes d'identité, nous nous assurons que personne ne peut voler l'identité d'une autre personne.

M. Nathaniel Erskine-Smith: Merci beaucoup.

J'ai lu des choses au sujet du système estonien. Lorsque des fonctionnaires ont accès aux renseignements d'un citoyen, cela est consigné. Pouvez-vous nous parler de la transparence du système? Je considérerais que ma vie privée est mieux protégée si je savais quand les fonctionnaires ont accès à mes renseignements et pourquoi. Dans quelle mesure est-ce que tout ça est documenté? À quoi cela ressemble-t-il en Estonie?

M. Raul Rikk: Voici comment le système fonctionne: lorsque je veux avoir accès aux services gouvernementaux, je dois accéder au portail de l'État, qui est, essentiellement, le site Internet où tous les services gouvernementaux sont répertoriés et présentés. Lorsque j'ouvre une session sur le portail de l'État, je vois en premier lieu les renseignements que le gouvernement possède sur moi: mon nom, si j'ai un permis de conduire ou une assurance-maladie et si je suis propriétaire ou non de propriétés immobilières ou de véhicules. Je peux voir tous les renseignements que le gouvernement possède à mon sujet.

Ensuite, je peux voir si le gouvernement a utilisé mes données de différentes façons. Par exemple, lorsque je conduis sur la route et qu'un policier vérifie mon numéro d'immatriculation, la voiture de patrouille ne m'arrête pas. Les policiers ne font qu'inscrire mon numéro d'immatriculation pour obtenir plein de renseignements à mon sujet, sur mon véhicule et d'autres choses. Lorsque les patrouilleurs procèdent ainsi, c'est immédiatement consigné. Je verrai plus tard dans le portail de l'État que ce policier a eu accès à mes données parce qu'il était en patrouille, et je vois exactement ce qu'il a fait. J'obtiens un aperçu de tout ça.

De la même façon, si je consulte un médecin et que le médecin regarde mes renseignements médicaux, ce sera consigné. J'en verrai plus tard un aperçu.

De cette façon, le gouvernement assure la transparence. Il me montre quelles données à mon sujet ont été consultées et par qui.

M. Nathaniel Erskine-Smith: Il ne me reste pas vraiment de temps, si je ne m'abuse, alors je cède mes 10 dernières secondes.

Le président: Nous allons maintenant passer à M. Gourde, pour cinq minutes.

[*Français*]

M. Jacques Gourde (Lévis—Lotbinière, PCC): Merci, monsieur le président.

Je vais poursuivre dans le même ordre d'idées et parler du portail de l'État.

Est-ce un portail à usages multiples où plusieurs ministères peuvent aller chercher de l'information avec ou sans le consentement du citoyen?

[*Traduction*]

M. Raul Rikk: Ce portail est conçu pour les citoyens et les résidents, aussi. Il y a une différence, si je peux m'exprimer ainsi. Différents organismes étatiques fournissent divers services électroniques. En tout, il y a environ 1 500 services électroniques distincts. Si vous voulez avoir accès à ces services, vous pouvez le faire directement par l'intermédiaire des sites Web des organismes. Si vous ne savez pas exactement quel genre de services sont offerts, vous pouvez ouvrir une session du portail de l'État. Tous les différents services de l'État y sont mentionnés.

● (0935)

[*Français*]

M. Jacques Gourde: D'autres organismes publics, privés ou commerciaux peuvent-ils aller chercher, dans ce portail de l'État, des renseignements qui pourraient les aider dans leur travail?

[*Traduction*]

M. Raul Rikk: Pouvez-vous préciser la question?

[*Français*]

M. Jacques Gourde: Oui.

Les informations à l'intérieur du portail de l'État peuvent-elles être consultées par les entreprises privées, les partis politiques ou d'autres personnes qui aimeraient les obtenir dans un but lucratif?

[*Traduction*]

M. Raul Rikk: Non, absolument pas. C'est l'information que seul moi je peux voir. Même les différentes institutions étatiques ne peuvent pas le voir. C'est seulement moi qui peux avoir mon portrait complet. Différents organismes étatiques peuvent seulement voir la portion dont ils sont responsables.

[*Français*]

M. Jacques Gourde: Dans l'ensemble des renseignements qu'on y retrouve, où se situe la limite des renseignements qui peuvent être considérés comme publics? Il y a le nom et l'adresse, mais cela s'arrête-t-il là? Par exemple, les numéros de téléphone publics, les numéros d'appareils mobiles ou les adresses de courrier électronique peuvent-ils être considérés comme des renseignements pouvant être divulgués à la population? Où se situe la limite?

[*Traduction*]

M. Raul Rikk: Les renseignements sont décrits de façon très précise dans la loi sur l'information publique. Nous avons une loi précise qui décrit quelle information est publique, laquelle est personnelle et laquelle est utilisée à des fins administratives. Tout le système, le système technique, est construit en fonction de cette loi.

[*Français*]

M. Jacques Gourde: On retrouve sur certains sites les numéros d'appareils mobiles de pratiquement tous les gens sur la planète, même si ces appareils sont la propriété privée de citoyens. Y a-t-il des mesures de contrôle face à ces sites spécialisés?

[*Traduction*]

M. Raul Rikk: Oui, exactement. Le contrôle est réalisé par l'inspectorat responsable de la protection des données, le même organisme que celui dont j'ai parlé tantôt. C'est lui qui a le pouvoir de superviser toutes les activités dans le monde numérique.

Mme Liia Hänni: En général, les renseignements contenus dans les bases de données gouvernementales ne sont pas des renseignements publics. Ce sont des renseignements personnels, qui nous concernent, mais, en Estonie, l'obtention de l'information des différentes bases de données est fondée sur mon code d'identification privé. C'est quelque chose de vraiment fondamental en ce qui a trait à l'identité numérique en Estonie, et, de plus, ce numéro spécial me donne accès à différentes bases de données qui contiennent des données à mon sujet. Les codes d'identification personnelle sont vraiment à la base du système d'échange de données et de protection de la vie privée estonien.

[*Français*]

M. Jacques Gourde: J'ai une dernière question. Devrait-on avoir une législation plus internationale? Les lois diffèrent d'un pays à l'autre et on ne peut pas garantir la même protection des renseignements de la vie privée des gens si on obtient des informations de la part d'un autre pays.

[*Traduction*]

M. Raul Rikk: Nous ne croyons pas connaître très bien la situation canadienne. Ce que nous pouvons dire, c'est que tout — du moins, ce que nous faisons dans le monde numérique — est fondé sur des lois qui ont été créées avec en tête le développement numérique.

● (0940)

Mme Liia Hänni: L'expérience estonienne, c'est que nous pouvons mieux protéger les données personnelles dans un environnement numérique que sous format papier. Si quelqu'un regarde mes documents papier, je ne peux pas le savoir, tandis que, dans le cas des transactions d'information numérique, elles sont visibles pour les citoyens. En fait, c'est quelque chose qu'il faut vraiment prendre en considération.

Le président: Merci, monsieur Gourde.

Nous passons maintenant, pour cinq minutes, à M. Saini.

M. Raj Saini (Kitchener-Centre, Lib.): Bonjour. Merci beaucoup d'être là.

Je veux poser une question plus générale au sujet de la politique étrangère.

D'après ce que j'ai compris, les attaques de 2007 ont été précipitées en partie par une décision nationale que vous avez prise, à Tallinn, soit de déplacer une statue. Corrigez-moi si j'ai tort. Pour poursuivre, un gouvernement souverain a pris la décision légitime de faire ce qu'il voulait sur son territoire au sujet de certains enjeux. L'attaque a découlé de ça.

À l'avenir, pour ce qui est de la politique étrangère, avez-vous été plus hésitant? Avez-vous tempéré vos propos? Est-ce que cela a modifié votre perception, d'une certaine façon, ce qui vous pousse à ne pas irriter certains pays? Est-ce que cela a changé votre vision d'une façon ou d'une autre?

M. Raul Rikk: Si je repense à l'époque de cet incident, je me demande quelles sont les leçons que nous avons tirées.

La première, c'est que nous devons coopérer plus étroitement avec les pays qui ont les mêmes valeurs que nous, essentiellement, tous les pays démocratiques. Pour ce qui est des pays qui n'aiment pas la façon démocratique de faire les choses, nous devons tout simplement garder à l'esprit que nous avons besoin d'autres solutions, des solutions techniques ou autres, afin d'empêcher que d'autres incidents se produisent.

Certainement, je crois que tout ça s'est reflété dans la politique étrangère, mais plus du point de vue positif en ce qui concerne la façon dont nous travaillons en coopération avec les pays démocratiques. Dans l'environnement de l'OTAN, l'Union européenne, il y a un très bon exemple: quelqu'un a mentionné tantôt que l'Estonie est un pays assez petit — et c'est vrai, seulement 1,3 million de personnes —, mais nous avons maintenant influencé toute l'Union européenne, dans la mesure où les mêmes principes que ceux dont nous avons parlé aujourd'hui sont déjà mis en oeuvre au sein de l'Union européenne, qui compte 500 millions de citoyens. Tout ça a assurément découlé de notre politique étrangère.

M. Raj Saini: Un des objectifs stratégiques de votre politique de cybersécurité, c'est la coopération internationale, et, depuis les attaques de 2007, certaines choses se sont produites. Déjà, l'OTAN a réalisé son propre examen. Je crois aussi que le gouvernement américain a envoyé des gens là-bas pour favoriser la protection contre les cyberattaques.

Cependant, lorsqu'on parle de coopération internationale — et je parle précisément de votre objectif, qui, selon moi, est très noble —, dans de nombreux cas, les pays qui sont prédisposés à concevoir des attaques, ne sont pas des pays démocratiques et ne possèdent pas les principes démocratiques dont nous jouissons. De quelle façon composez-vous avec cette situation?

Vous avez parlé de l'Union européenne — et c'est parfait, puisque tous les pays sont démocratiques —, mais lorsqu'il est question de coopération internationale, beaucoup des attaques qu'essuieront certains États souverains ne viendront pas de pays démocratiques ou stables.

De quelle façon abordez-vous cet enjeu lorsqu'un des principes fondateurs dans votre document sur la cybersécurité, c'est la coopération internationale?

M. Raul Rikk: Nous le faisons par l'intermédiaire de l'Union européenne, parce que tous ces pays auxquels vous avez probablement fait référence sont très grands. Ils ne discutent tout simplement pas de ces choses avec nous, alors la seule façon de composer avec ces pays, c'est par l'intermédiaire de la politique étrangère de l'Union européenne.

En outre, disons que la coopération internationale ou la politique étrangère dans ce domaine permet d'assurer, environ, probablement 30 % de la sécurité, mais la plupart des choses que nous pouvons faire restent de nature technique. La mise en place de nouvelles technologies assure la sécurité pour nous dans le cyberespace, et grâce à la politique étrangère, nous gérons seulement la composante que nous ne pouvons pas gérer techniquement.

● (0945)

Le président: Il y a un léger délai, alors si vous avez une dernière...

M. Raj Saini: C'est parfait.

Le président: Merci, monsieur Saini.

Nous passons maintenant à M. Kent pour cinq minutes.

L'hon. Peter Kent: Merci, monsieur le président.

Pour revenir sur ce que vous avez dit concernant le fait qu'il n'y a eu aucun cas de vol d'identité — et je crois que c'est vraiment impressionnant —, je crois savoir que, il y a plusieurs mois, quelque 760 000 certificats personnels ont été suspendus, pas parce qu'il y avait eu atteinte, mais en raison d'une évaluation de la menace qui avait permis de conclure que les puces dans les cartes étaient peut-être défectueuses ou vulnérables.

Pouvez-vous nous expliquer ce qui s'est produit à ce moment-là?

Je crois savoir que ces puces sont fabriquées non pas en Estonie, mais en Suisse.

M. Raul Rikk: Oui.

Nous avons découvert que l'entreprise produisant les cartes d'identité pour nous n'avait pas utilisé le meilleur chiffrement possible. Les cryptoprocesseurs sur les cartes n'avaient pas été produits comme le prévoyait le contrat. Essentiellement, ils n'étaient pas assez bons. Ces puces ont été produites par l'entreprise suisse Gemalto, et les puces précises avaient quant à elles été fabriquées par l'entreprise allemande Infinia.

Dans ce dossier, nous n'avons pas été les seuls touchés: il y avait aussi l'Espagne, la Slovaquie, Microsoft et tous les autres intervenants du secteur privé et du secteur public utilisant les mêmes puces. Cela concernait les puces fabriquées durant une certaine période, de la fin de 2014 à 2016.

En ce qui a trait à l'Estonie, c'était un incident majeur, parce que cela concernait près de la moitié des cartes d'identité utilisées au pays. On pourrait dire que la moitié de la population était théoriquement menacée.

Je dois rappeler que rien ne s'est produit, parce que nous avons éliminé cette vulnérabilité et réagi très rapidement. Essentiellement, nous avons mis au point une solution en deux mois, et nous avons commencé à délivrer de nouveaux certificats immédiatement après. Nous n'avons pas eu d'incident de sécurité, mais cela a soulevé la préoccupation précise de savoir de quelle façon nous allions aborder le problème à l'avenir et la façon d'éviter d'acheter un produit certifié pour ensuite découvrir que la certification était erronée.

L'hon. Peter Kent: Voilà qui m'amène à une autre question.

Vu l'évolution rapide des technologies et l'évolution des cybermenaces, à quelle fréquence prévoyez-vous devoir délivrer de nouveaux certificats assortis d'une nouvelle technologie de chiffrement sécuritaire?

M. Raul Rikk: La mise à jour a été effectuée sur Internet, de la même façon que nous mettons à jour nos ordinateurs personnels. Du point de vue des ressources, ce n'était pas très important. Cela signifiait seulement que chaque personne devait brancher sa carte d'identité dans son ordinateur personnel pour mettre à jour le certificat. Les gens doivent le faire de toute façon tous les deux ans, alors, dans ce cas-ci, ils ont dû le faire plus rapidement. Du point de vue des ressources, ce n'était pas un grand problème, le problème, c'était qu'il existait une possible vulnérabilité que nous ignorions.

● (0950)

L'hon. Peter Kent: Quelles sont les considérations liées aux coûts en ce qui concerne le certificat individuel et la puce utilisée, la technologie qu'elle permet de gérer?

M. Raul Rikk: Je n'ai pas le calcul du coût des certificats, mais la carte d'identité munie d'un cryptoprocesseur, des certificats et de tout le reste coûte 20 euros par personne. Nous n'avons pas eu à changer les cartes d'identité; seulement les certificats ont dû être modifiés, alors j'imagine que cela a coûté peut-être un euro par personne.

L'hon. Peter Kent: Merci.

Le président: Merci, monsieur Kent.

Nous passons maintenant à M. Picard pour cinq minutes.

M. Michel Picard: Merci.

Puisque nous avons seulement cinq minutes, passons directement aux questions.

La qualité d'un système tient aux personnes qui le gèrent. De quelle façon gérez-vous le risque de coup monté de l'intérieur, du point de vue des ressources humaines?

M. Raul Rikk: Encore une fois, nous gérons ces vulnérabilités internes à l'aide des cartes d'identité. En ce qui concerne les choses que différentes personnes font dans le cyberenvironnement, il y a un registre. Tout est consigné, et nous pouvons examiner les registres ultérieurement. Si l'administrateur, par exemple, veut apporter un changement dans le système, il doit s'identifier lui-même avec sa carte d'identité. C'est de cette façon que nous prévenons tout ça. C'est une des mesures.

La deuxième mesure, c'est que nous ne possédons pas une grande base de données. Comme vous le voyez sur la diapositive, il y a des centaines de bases de données distinctes relevant de divers organismes, et différentes personnes ont accès à ces bases de données. Tout est décentralisé et rien n'est concentré, alors, si quelqu'un obtient l'accès à certains systèmes, qu'il peut causer des préjudices à ces systèmes, il peut seulement le faire dans une mesure limitée. Il ne peut pas provoquer la défaillance de tout le système.

M. Michel Picard: Au sujet du fait que vous avez des bases de données distinctes, j'ai deux choses à dire. Premièrement, du point de vue des enquêtes, nous créons de plus en plus de logiciels permettant de créer des ponts entre les différentes bases de données afin de pouvoir créer des relations, parce que la qualité et l'efficience d'une base de données dépendent de sa capacité à créer des liens. En séparant les bases de données, créez-vous de redondances et, par conséquent, est-ce que cela ralentit le processus de recherche ou d'enquête?

M. Raul Rikk: Pour être honnête, je ne suis pas sûr d'avoir compris votre question.

M. Michel Picard: D'accord, je vais la reformuler.

Je vais vous donner un exemple, et je ne fais pas la promotion d'un produit, mais je veux savoir de quelle façon tout cela fonctionne.

Du point de vue des enquêtes, i2 Solutions a mis au point des « ponts » pouvant réunir des données de différentes bases de données ensemble, parce que la qualité d'une bonne base de données, c'est sa capacité à créer des liens, grâce aux noms, aux adresses, à l'heure, aux tendances, aux amis et ainsi de suite. En créant des bases de données distinctes, faut-il assurer une redondance? De plus, passer d'une base de données à une autre, du point de vue d'une enquête ou du point de vue de la recherche, ralentit beaucoup le processus.

M. Raul Rikk: Permettez-moi d'expliquer de quelle façon le système fonctionne. Cela répondra peut-être à votre question.

Sur la diapositive, on voit les différentes bases de données. 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 oeil 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 que vous voyez sur la diapositive. 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.

● (0955)

M. Michel Picard: J'ai une dernière question concernant le vol d'identité.

Le problème, lorsqu'on enquête sur un crime numérique, c'est de savoir qui était devant l'écran et qui tapait sur le clavier. Pour ce qui est de l'utilisation d'une carte, de quelle façon pouvons-nous nous assurer que la personne utilisant la carte est bien son propriétaire?

M. Raul Rikk: C'est bien sûr une très bonne question, mais il n'y a aucune façon d'être sûr à 100 % ni d'identifier la personne. Notre police utilise différentes techniques pour régler les cybercrimes. C'est en partie grâce à la carte d'identité, mais, bien sûr, la carte d'identité elle-même ne donne pas une garantie à 100 %, alors nous devons utiliser d'autres techniques aussi lorsque nous enquêtons sur de tels dossiers.

M. Michel Picard: Merci.

Le président: Merci, monsieur Picard.

Je tiens à souligner le retour de M. Cullen, un ancien membre. Vous avez seulement trois minutes, ce n'est rien de personnel.

M. Nathan Cullen (Skeena—Bulkley Valley, NPD): Oui, oui...

Des voix: Ha, ha!

M. Nathan Cullen: Oui, c'est ce que j'ai remarqué, monsieur le président.

Le président: Je voulais tout simplement en informer les autres membres du Comité aussi. Nous avons beaucoup de temps.

M. Nathan Cullen: Nous avons beaucoup de temps, mais je n'ai pas droit à beaucoup de temps. Est-ce que c'est ce que vous essayez de me dire? Je comprends.

Le président: Nous avons jusqu'à 10 h 45, donc, après la période de questions de trois minutes accordée à M. Cullen, nous allons tout simplement faire un tour de table.

Allez-y, monsieur Cullen.

M. Nathan Cullen: Je serai rapide.

Merci aux représentants. Je suis désolé si je n'étais pas là pour la première partie de votre témoignage, et je m'excuse donc si je vous pose des questions auxquelles vous avez déjà répondu.

Permettez-moi de commencer par une question. Êtes-vous en mesure de répondre à des questions sur le système de vote électronique utilisé en Estonie ou êtes-vous préparés à le faire? Puis-je présumer que, essentiellement, vous utilisez le même réseau et le même système de sécurité que pour les cartes numériques?

M. Raul Rikk: De façon générale, oui, je suis prêt à répondre aux questions. Cependant, bien sûr, si vous posez des questions trop précises, je ne pourrai pas y répondre.

M. Nathan Cullen: À part les renseignements précis, je me questionne sur les récentes révélations, pas seulement au sujet de Facebook, mais au sujet des atteintes assez importantes à la protection des données que nous constatons à l'échelle mondiale. Aux États-Unis et aussi, ici, au Canada, tant des entreprises traditionnelles que des entreprises électroniques et des experts dans le domaine n'ont pas réussi à assurer la protection de leurs données. Nous parlons là d'entités qui ont de très, très bonnes raisons financières de le faire. J'inclus ici Uber, Yahoo, Target, Sony, le gouvernement américain et le gouvernement canadien.

Pour revenir au vote, il y a eu certaines critiques quant à la sécurité de votre système de vote — c'est ce que nous avons appris dans un témoignage devant un comité différent, ici — en raison de la capacité de violer le système de vote électronique puis de couvrir ses traces, si je peux dire, ce qui est une grave menace pour les pays démocratiques.

Vu la participation d'autres États et d'autres intervenants politiques nationaux, qu'est-ce que l'Estonie a fait récemment pour rendre son système de vote électronique plus sécuritaire, afin que les élections restent libres et équitables?

M. Raul Rikk: Ce qui est arrivé, récemment, c'est que lorsque je vote, après avoir voté je peux... Par exemple, si j'utilise un ordinateur, je peux vérifier si mon vote s'est rendu à destination ou non. Je peux le vérifier sur mon téléphone mobile. Il y a deux façons de s'assurer que mon vote s'est rendu là où il devait se rendre.

En ce qui a trait à l'ensemble du système de vote et de la sécurité de ce système, nous utilisons de nombreuses technologies et procédures différentes. Je dois dire que les critiques sont toujours les bienvenues, mais elles ne sont pas toujours très pertinentes.

Par exemple, très souvent les critiques qu'on entend, c'est un peu comme la personne qui affirme qu'allumer une chandelle sur une table peut déclencher un incendie dans l'immeuble. Nous utilisons tous des chandelles, surtout durant le temps des Fêtes, et il y a très, très rarement des incendies. Bien sûr, lorsqu'on allume une flamme, sur une table, il y a toujours un risque d'incendie.

En grande partie, les critiques contre le système de vote sont du même type. Les gens affirment que quelque chose pourrait se produire, mais, en réalité, ce n'est pas le cas. Il n'y a pas eu d'incident lié au système de vote. Il y a toujours de la supervision et du contrôle, et nous le faisons de différentes façons. Si nous mettons en oeuvre toutes les mesures, nous pouvons dire que le système est sécuritaire. Bien sûr, il y a toujours des possibilités, il y a toujours un truc.

● (1000)

Le président: Merci, monsieur Cullen.

Allez-y, madame Hänni.

Mme Liia Hänni: J'étais membre du comité des affaires constitutionnelles lorsque nous avons décidé initialement de passer au vote sur Internet. Bien sûr, il y avait des préoccupations, mais le système de vote électronique est constamment mis à niveau pour éliminer les différents risques que l'on court.

Essentiellement, dans le système estonien, il n'y a pas eu ce genre d'atteinte ou d'interférence dans le cadre du processus de vote et, pour cette raison, les citoyens estoniens utilisent de plus en plus Internet pour voter. La confiance est déjà là. Bien sûr, les technologies sont toujours assorties de certains risques, mais, comme je l'ai dit, il faut être prêt à composer avec ces risques sans arrêter d'aller de l'avant. C'est mon point de vue politique.

M. Raul Rikk: Je veux formuler très rapidement un commentaire sur le fait que le système de vote n'est pas totalement distinct de ce dont nous avons déjà parlé. Il reste fondé sur les cartes d'identité émises et dotées d'un très bon système de chiffrement.

Le président: Merci à vous deux.

Nous allons maintenant y aller pour sept minutes ou moins. Je suis sûr que ce sera probablement moins.

Pour commencer, nous entendrons M. Kent, qui est sur la liste, M. Baylis et M. Erskine-Smith. Si vous voulez ajouter votre nom, il nous reste environ 40 minutes.

L'hon. Peter Kent: Merci, monsieur le président. J'ai seulement une question, qui est liée aux dernières remarques sur le système de vote.

Avez-vous mesuré le niveau d'acceptation publique du système de données électroniques qui a été mis en place et qui continue d'être utilisé, malgré les défis occasionnels, ici et là, comme le besoin de reprogrammer 750 000 certificats? Avez-vous réalisé un sondage pour évaluer l'acceptation publique du système ou la satisfaction relativement au système?

Mme Liia Hänni: De façon générale, les Estoniens utilisent le système de gouvernement numérique et je crois que c'est fondamental, parce que s'il n'y a pas d'utilisation du gouvernement numérique pour le renforcer...

Pour ce qui est du vote sur Internet, vous pouvez voir dans ces diapositives la croissance constante du nombre d'électeurs qui votent en ligne. Nous avons tenu les élections locales l'automne dernier, et environ le tiers des personnes qui ont participé aux élections ont voté en ligne. Cependant, en Estonie, comme je l'ai dit, il y a, bien sûr, des gens qui s'opposent encore au vote sur Internet, parce qu'il n'y a pas de garantie à 100 % qu'il n'y aura pas de problème. Comme vous pouvez le voir, cela fait partie du processus normal en Estonie, mais les gens peuvent tout de même choisir de quelle façon ils votent.

En Estonie, les gens croient que la gouvernance numérique est une bonne chose, et la principale préoccupation concerne les progrès que nous faisons. Pouvons-nous saisir toutes ces nouvelles occasions qu'offre la technologie, comme l'intelligence artificielle, par exemple?

L'hon. Peter Kent: De quelle façon composez-vous avez les capacités et la confiance des générations plus âgées, qui ne sont pas autant sur Internet et qui ne connaissent peut-être pas autant les nouvelles technologies?

Mme Liia Hänni: Je crois que vous parlez des gens de ma génération, parce que je fais partie moi aussi du bel âge.

Des voix: Ha, ha!

L'hon. Peter Kent: C'est ma génération aussi.

Mme Liia Hänni: C'est important de comprendre que la génération âgée peut encore apprendre et saisir de nouvelles occasions. En Estonie, le gouvernement a aussi mis en place plusieurs programmes spéciaux pour encourager les plus vieux à participer à la société de l'information. Dans le cadre de ces programmes, on regarde le monde et on envoie des autobus dans différents villages estoniens et on forme des aînés afin qu'ils utilisent des ordinateurs, mais je crois que notre jeune génération, qui est en ligne à 100 %, peut aussi fournir un bon soutien aux grands-parents.

● (1005)

M. Raul Rikk: Enfin, nous avons mesuré la façon dont les plus jeunes et les plus vieux abordent le processus de vote. Les statistiques sont assez intéressantes. Elles nous apprennent que les jeunes prennent plus de temps pour voter, et que les aînés le font plus rapidement et de façon plus efficiente. Ils ne naviguent pas sur le site Web de vote, mais suivent exactement la procédure qu'ils sont censés suivre, tandis que les plus jeunes ne font que naviguer et n'appuient pas toujours aux bons endroits. Cela nous montre que les membres de la jeune génération savent très bien comment jouer à Minecraft et comment utiliser Facebook, mais ils ne savent pas nécessairement de quelle façon utiliser leur carte d'identité et suivre des procédures officielles.

Le président: C'est intéressant.

J'aimerais préciser... il y a seulement trois noms sur la liste. Je pensais avoir vu plus de mains levées. J'ai seulement M. Baylis, M. Erskine-Smith et M. Picard. Nous aimerions Mme Vandenbeld, aussi. Vous pouvez tout simplement lever la main si je n'ai pas inscrit votre nom. D'accord, alors il y a Mme Murray et M. Cullen à nouveau.

D'accord. Passons à M. Baylis, pour un maximum de sept minutes.

M. Frank Baylis (Pierrefonds—Dollard, Lib.): Merci.

J'ai quelques questions pour vous, madame Hänni. J'ai regardé cette excellente diapositive et la façon dont l'Estonie en est venue à mettre en place ce système très complet, mais, évidemment, vous n'avez pas commencé là. Si nous envisageons de construire quelque chose du même genre, par où devons-nous commencer? Est-ce le registre de la population, l'identifiant unique? De quelle façon faudrait-il procéder?

Mme Liia Hänni: C'est une très bonne et très importante question.

Je crois que ce qui est vraiment nécessaire, c'est un système d'identification électronique. En Estonie, il est fondé sur l'identifiant unique des citoyens. Je sais que, au Canada, il n'y a pas de registre de la population pour tout le pays, seulement pour les provinces, alors vous devriez définitivement réfléchir à mettre en place un solide système d'identité pour vos citoyens.

Ensuite, puisque vous avez un très grand nombre d'ensembles de données qui ne sont pas connectés les uns aux autres, les ensembles appartenant à différents organismes, vous devriez réfléchir à la façon de créer un système dans lequel les données circuleront, et, une fois que vous aurez cette capacité de communiquer les données, au besoin, alors, bien sûr, il faudra mettre en place un système pour protéger l'intégrité de ces données.

En Estonie, grâce à X-Road, nous avons différentes installations techniques pour protéger les données, mais, essentiellement, au moment de connecter les bases de données à X-Road, il y a une vérification des enjeux liés à la protection des renseignements personnels, des vérifications liées à la sécurité et un pouvoir très défini, et une institution différente qui s'assure que le système de données fonctionne de façon appropriée.

Vous avez déjà de très bons systèmes, beaucoup de données en ligne, et une bonne vision quant au gouvernement ouvert, alors je crois que c'est une question de volonté politique de prendre ces nouvelles décisions de base afin non seulement d'avoir de bons systèmes d'information distincts, mais de considérer le Canada, l'environnement physique canadien, comme un seul système. Selon moi, c'est le travail qui vous attend maintenant.

● (1010)

M. Frank Baylis: Lorsque vous avez mis sur pied votre système, y avait-il des préoccupations? Je sais que vous avez parlé de la façon dont tout ça s'intègre à la démocratie en tant que telle. Avez-vous eu des préoccupations à dissiper? Vous avez mentionné l'une des préoccupations, le vote électronique chez les aînés, mais, de façon générale, lorsque vous alliez de l'avant et mettiez en place cette société extrêmement numérisée, de quelle façon avez-vous obtenu l'adhésion de la population?

Mme Liia Hänni: Je crois que la population estonienne voyait très positivement l'utilisation des technologies. Même lorsque nous avons mis en place le vote électronique, une grande partie de la société n'utilisait pas Internet, mais même les gens qui n'utilisaient pas Internet avaient une attitude très positive à cet égard. Selon moi, nous n'avons pas vu ce genre d'opposition à l'utilisation des technologies en Estonie.

Ce qui était bien, ce que le Parlement a fait, c'est de mettre en place des lois de base, comme celles sur l'identité numérique entrée en vigueur en 2001. La signature numérique est le service électronique le plus utilisé en Estonie. Nous n'avons plus besoin de signer des documents papier maintenant. Nous utilisons des signatures numériques, et c'est là une énorme économie de ressources, de temps et d'argent que permet cette nouvelle méthode actuellement.

La mise en place du gouvernement numérique estonien ne s'est pas faite dans le cadre d'un seul projet. C'était un processus étape par étape, mais nous avons pris les bonnes décisions au bon moment. L'utilisation de l'identité numérique, la loi et la technologie pour le système X-Road et cette couche d'interopérabilité dont nous nous sommes dotés étaient tous nécessaires, parce que nous avions en Estonie une situation similaire à celle du Canada. Il y avait différents ensembles de données qui ne travaillaient pas ensemble, et la couche d'échange d'information X-Road était nécessaire pour surmonter cette situation. Pour cette raison, nous n'avons plus besoin de compter combien de services électroniques nous offrons, et c'est facile d'en ajouter de nouveaux, de réunir les renseignements et les données que contiennent nos systèmes.

En Estonie, le gouvernement peut seulement utiliser mes données conformément à la loi. Les données ne peuvent pas être utilisées par le gouvernement sauf si la loi donne le pouvoir aux institutions gouvernementales de demander et d'utiliser mes données, et c'est très important et différent de ce que font les entreprises privées, où l'obtention du consentement peut être la force motrice menant à l'utilisation de mes données.

M. Frank Baylis: J'ai une autre question. Il est évident que vous avez consulté un certain nombre de pays différents sur certains sujets, et les gens sont venus voir la situation en Estonie pour en tirer des leçons. Y a-t-il des leçons sur ce que nous devrions éviter, certains dangers, certains pièges, dont nous devons être au fait si nous entreprenons un processus similaire, des erreurs que vous avez peut-être vu d'autres pays faire?

Mme Liia Hänni: D'après notre expérience, tous les pays avec lesquels nous travaillons veulent de bons services électroniques, mais, pour avoir un système, les gouvernements doivent pouvoir apporter des changements assez radicaux aux attitudes qu'ils ont eues jusqu'à ce moment-là. La mise en place d'un gouvernement numérique n'est pas tant une question de technologies ou de nouveaux systèmes d'information, qu'une question d'innovation, de coopération novatrice entre les différents ministères. L'interopérabilité est technologique, mais cela tient aussi à la façon dont on élimine les cloisons au sein de l'administration étatique, à la façon dont on s'assure que toutes les organisations travaillent en collaboration. C'est le défi le plus important auquel de nombreux pays sont encore confrontés.

Le président: Merci, monsieur Baylis.

Nous passons à M. Erskine-Smith.

M. Nathaniel Erskine-Smith: Merci beaucoup.

J'ai deux ou trois questions très courtes, et deux ou trois plus longues. Je vais commencer par les questions courtes.

Nous avons précédemment parlé de la façon dont, si des fonctionnaires ont accès à l'information, il y a un dossier, et c'est transparent. Quelle est la pénalité si des fonctionnaires ont accès de façon inappropriée à l'information?

● (1015)

M. Raul Rikk: Dans ce cas, il n'y a pas de pénalité prédéfinie. Chaque fois que ce genre d'incident se produit, il y a une enquête, puis un tribunal décide quelle doit être la sanction.

M. Nathaniel Erskine-Smith: Tout dépend de la gravité de l'inconduite. D'accord.

Notre commissaire à la protection des renseignements personnels a récemment parlé dans les médias des inquiétudes au sujet des services gouvernementaux numériques, mais il semblait que sa principale préoccupation — il viendra nous voir à une date ultérieure — c'était le fait que le gouvernement recueille des renseignements publics sur les citoyens, que ce soit sur Facebook ou ailleurs.

Est-ce que l'Estonie s'adonne à de telles pratiques? Est-ce que cela fait partie du gouvernement numérique?

M. Raul Rikk: Notre gouvernement ne recueille pas de données sur Facebook. Toutes les données que notre gouvernement recueille, comme Liia l'a mentionné, sont recueillies conformément à la loi et directement auprès des propriétaires de données, les citoyens.

M. Nathaniel Erskine-Smith: Excellent.

Je peux très bien imaginer que certains citoyens âgés de ma circonscription, qui n'utilisent peut-être pas autant Internet que moi ou d'autres le faisons, pourraient craindre dans une certaine mesure que le service à la clientèle passe complètement en mode numérique et qu'ils perdent tous les services qu'ils ont ou qu'ils ne puissent plus parler à quelqu'un au téléphone pour obtenir des services auxiliaires visant à les aider à avoir accès à l'environnement numérique.

Quelle a été l'expérience estonienne? Si j'ai de la difficulté à obtenir un service gouvernemental numérique, vers qui est-ce que je peux me tourner?

M. Raul Rikk: Si vous avez de la difficulté, vous pouvez toujours vous tourner vers un centre de service gouvernemental et obtenir de l'aide là-bas, mais les solutions ou les services numériques font en sorte que, si je veux le faire sur Internet, je n'ai pas à me rendre dans un centre de service gouvernemental. Je peux faire toutes mes opérations et interagir avec le gouvernement, peu importe où je suis, au Canada, en Australie ou en Nouvelle-Zélande. Peu importe. Tant que j'ai une connexion Internet, je peux utiliser tous les services accessibles.

M. Nathaniel Erskine-Smith: Nous n'en avons pas discuté. Nous avons vu le système X-Road. Nous avons pu constater le principe de non-chevauchement des bases de données. Nous avons votre liste des diverses façons dont vous protégez la sécurité et la confidentialité. De quelle façon la chaîne de blocs est-elle utilisée pour protéger la confidentialité des citoyens estoniens?

M. Raul Rikk: C'est une très bonne question, parce qu'on a beaucoup parlé au cours des dernières années de la chaîne de blocs. Tout le monde en parle, mais nous l'utilisons pour sécuriser les signatures numériques. Nous avons commencé à utiliser la logique de la chaîne de blocs avant que le nom soit même inventé. Lorsque nous avons délivré notre première carte d'identité, en 2002, la logique de la chaîne de blocs était déjà appliquée dans le système.

Essentiellement, ce que nous faisons, c'est que nous mettons l'ancienne signature numérique ou les empreintes des signatures numériques dans la nouvelle signature numérique. Essentiellement, nous créons un lien entre les différentes signatures numériques afin que, peu importe ce qui se passera du point de vue du chiffrement, à l'avenir, nous pourrons encore bénéficier du lien sécurisé associé aux signatures numériques.

M. Nathaniel Erskine-Smith: Pour ce qui est des autres pays qui adoptent un gouvernement plus numérique, j'ai lu que la Finlande veut tout simplement utiliser X-Road. D'autres pays mettent au point leur propre système.

La Finlande est-elle le seul pays qui veut utiliser la même technologie que celle sur laquelle les services numériques estoniens sont fondés? Est-ce que d'autres pays font la même chose? De quelle façon cela fonctionne-t-il?

M. Raul Rikk: C'est ce sur quoi nous travaillons chaque jour. La Finlande est un des pays. Nous l'avons fait dans d'autres pays aussi, même si on ne l'a pas beaucoup fait en Europe, mais tout dépend des approches des différents pays en matière d'échange de données. Nous croyons que c'est la meilleure solution pour lier les différentes bases de données. Aucune des organisations n'a besoin de changer ce qu'elle a déjà; elles doivent tout simplement ajouter une couche de sécurité sur les systèmes actuels.

Je ne peux pas vous dire pourquoi la plupart des pays n'ont pas commencé à l'utiliser.

M. Nathaniel Erskine-Smith: Nous n'avons pas vraiment discuté de la collaboration avec le secteur privé. Vous pourriez peut-être nous fournir des explications à ce sujet. Je vois dans le tableau que le citoyen est à côté du gouvernement, qui est à côté des entreprises.

De quelle façon les renseignements privés et personnels des personnes sont-ils communiqués aux entreprises du secteur privé dans ce contexte? Quels secteurs différents ont accès à cette information par l'intermédiaire des services gouvernementaux numériques? Quelles sont les pratiques exemplaires pour assurer la protection des renseignements personnels des gens?

● (1020)

M. Raul Rikk: 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. De façon générale, le secteur privé fournit des services. Il possède certaines données au sujet des citoyens et il fournit ces données pour assurer la prestation d'un service gouvernemental.

Par exemple, il y a la déclaration de revenus électronique. Les banques ont des renseignements au sujet des revenus personnels. Les banques créent les rapports. Je peux me tourner vers mon service bancaire et permettre à ma banque d'envoyer ces données à l'agence du revenu de l'Estonie, qui prend cette information et l'intègre dans ma déclaration de revenus. Je n'ai pas à le faire. C'est ainsi que ça fonctionne. Le secteur privé génère certains renseignements, et il peut les fournir au gouvernement de façon sécurisée par l'intermédiaire de X-Road.

Le président: Merci.

Nous passons maintenant à M. Cullen.

M. Nathan Cullen: Merci.

Y a-t-il des exigences dans la loi quant à l'endroit où les serveurs doivent être situés? Doivent-ils tous se trouver sur le territoire estonien? Ou se peut-il que certains de vos partenaires du secteur privé ou certains services gouvernementaux soient situés à l'extérieur du pays?

M. Raul Rikk: Il y a des limites en ce qui a trait aux services essentiels ou cruciaux. Les systèmes bancaires sont l'un d'eux. Par exemple, après les attaques de 2007, certaines banques suédoises voulaient prendre des données de l'Estonie et les conserver en Suède. Le Parlement estonien a établi par règlement que les données concernant les renseignements bancaires devaient être conservées en Estonie. Les données peuvent être conservées en Suède ou dans d'autres pays si les intervenants le désirent, bien sûr elles doivent être chiffrées, mais l'information doit aussi être en Estonie de façon à ce que, si quelque chose se produit au chapitre de la connectivité Internet, cela n'influera pas sur la prestation du service.

M. Nathan Cullen: Vous en avez peut-être déjà parlé, mais je viens de lire tout ce que l'Estonie a fait jusqu'à présent du point de vue des services gouvernementaux électroniques. Il est mentionné à quelques reprises le gouvernement de coalition favorable au numérique en 2001, mais je ne comprends toujours pas. Y a-t-il eu une élection en 2001?

Nous sommes en politique. Les gens peuvent parler de la « chaîne de blocs » et je peux hocher la tête, mais je n'ai en fait aucune idée de ce dont on parle. Je peux lire tout ça six fois et tout de même ne pas comprendre ce dont on parle. Dans tous les cas, il y avait une certaine volonté politique au tournant du siècle pour lancer l'Estonie dans cette voie. Y a-t-il eu un événement politique, une crise économique? Quelque chose a-t-il facilité ce genre de consensus politique qui vous a menés à prendre une mesure d'aussi longue haleine et assez audacieuse?

Mme Liia Hänni: Le processus a commencé plus tôt dans le cadre du processus de mise sur pied de l'Estonie. En fait, on partait de rien après l'occupation soviétique. Nous avions cette vision et une solide volonté politique de créer un État moderne et de miser sur nos technologies. Nous avions des gens qui connaissaient beaucoup les technologies et aussi des politiciens qui croyaient que ces technologies pouvaient nous aider dans nos efforts de modernisation et de création d'un État vraiment moderne. Il n'y avait pas d'opposition politique à l'utilisation des technologies.

Il y a eu de l'opposition lorsque nous avons présenté les cartes d'identité numérique, en 2001. Il y a eu un débat au sein du comité constitutionnel. Certains membres du comité ont demandé pourquoi nous avions besoin de cette identité numérique, quels étaient les genres de services que le gouvernement allait offrir. C'était difficile de leur expliquer à ce moment-là ce que nous voulions faire exactement avec l'identité numérique, mais nous avions en tête que la numérisation allait se poursuivre et que tôt ou tard, il allait être nécessaire de pouvoir s'identifier dans le monde numérique. Nous avons pris cette très bonne décision de ne pas rendre la carte d'identité numérique volontaire. On est obligé en Estonie d'avoir une carte d'identité numérique. Tous les citoyens et résidents de l'Estonie doivent l'avoir.

● (1025)

M. Nathan Cullen: Je comprends. Je vous remercie de cette réponse.

Je veux revenir à la question d'un gouvernement qui s'adonnera à l'exploration de données à l'extérieur des services gouvernementaux directs en tant que tels.

Je pourrais comprendre qu'un gouvernement dise que, pour comprendre les répercussions d'un programme de vaccination ou d'un programme de nature économique offert, l'un des meilleurs ensembles de données qui existent pour connaître ce que les gens disent au sujet d'un programme ou d'un service ou d'une politique gouvernementale précise, ce sont les médias sociaux. En tant que gouvernement, nous réalisons des sondages tout le temps, mais nous savons aussi que les sondages permettent une compréhension limitée. Beaucoup de personnes passent beaucoup, beaucoup plus de temps en ligne, et plus de personnes discutent de politiques ou de ce qui se passe localement dans l'environnement des médias sociaux.

Vous avez dit précédemment que le gouvernement ne procède pas à une telle exploration de données sur le site de média social Facebook. Il y en a beaucoup d'autres, et il y en a d'autres qui sont plus populaires en Estonie. Pourquoi pas? Vu les motivations bien intentionnées — je ne parle même pas de motivation viles — d'un gouvernement de procéder ainsi, et vu les violations simplement au sein de Facebook en tant que tel, on pourrait imaginer un gouvernement qui passerait un contrat lui permettant de comprendre les répercussions de sa dernière politique en matière de garde d'enfants grâce à l'exploration de données et en découvrant ce que les gens disent à ce sujet sur Facebook, Twitter ou Instagram.

Mme Liia Hänni: En Estonie, les médias sociaux sont encore beaucoup utilisés dans le secteur public, mais c'est essentiellement pour communiquer avec les citoyens. Ce n'est pas exactement nécessaire d'aller voir sur Facebook ce que les gens pensent du gouvernement et des services gouvernementaux. Nous sommes très ouverts à une coopération directe avec notre gouvernement, plutôt que de passer par Facebook.

Il y a assurément beaucoup de renseignements sur Facebook. Je ne dénigre pas l'occasion d'utiliser cette information pour améliorer les services, par exemple, ou mieux comprendre des processus politiques, mais, à coup sûr, ce ne doit pas servir à faire du profilage des citoyens afin d'obtenir un certain pouvoir politique ou à des fins politiques. Je crois que c'est ce dont vous parlez.

M. Raul Rikk: Le profilage n'est pas permis conformément à la nouvelle réglementation de l'Union européenne sur la protection des données. Essentiellement, c'est interdit.

M. Nathan Cullen: Je suis désolé. Je n'ai pas entendu la première partie de votre phrase. Qu'est-ce qui est interdit par la nouvelle réglementation de l'Union européenne?

Mme Liia Hänni: Le profilage.

M. Raul Rikk: Le profilage des personnes.

M. Nathan Cullen: Le profilage des personnes par les gouvernements est interdit dans la réglementation de l'Union européenne. Je suis désolé, je veux bien comprendre. Est-il illégal pour les gouvernements de procéder au profilage des citoyens?

M. Raul Rikk: Oui. Essentiellement, on ne peut pas faire de profilage des gens par l'intermédiaire des médias sociaux.

M. Nathan Cullen: Ce serait utile pour le Comité d'avoir accès à ce règlement, parce que je ne l'ai pas. Je ne sais pas si d'autres membres du Comité suivent les lignes directrices réglementaires de l'Union européenne en matière d'Internet, mais si votre gouvernement pouvait nous le fournir, c'est quelque chose que j'aimerais bien consulter.

Merci, monsieur le président.

Le président: Merci, messieurs.

Nous passons maintenant à Mme Vandenbeld, puis à Mme Murray.

Il reste un peu moins de temps. Il reste encore cinq minutes d'affaires du Comité à régler, alors il faudra mettre fin à la discussion à ce moment-là.

Allez-y, madame Vandenbeld.

Mme Anita Vandenbeld: Liia, vous avez mentionné que cela s'inscrit dans la reconstruction de l'État estonien. C'est un processus qui remonte à quelques décennies maintenant, et, dès le départ, vous avez imaginé en arriver là où vous êtes aujourd'hui.

Lorsqu'on a des architectures très complexes qui n'ont pas été conçues ni bâties étape par étape en ce sens, est-il plus difficile de prendre les architectures actuelles et de faire ce que vous avez fait, ou de le faire, par exemple, dans une nouvelle démocratie et de recommencer à zéro? Y a-t-il des défis associés au fait qu'il y a déjà des services gouvernementaux et déjà un processus de numérisation en cours dans divers ministères où il y a déjà une centralisation? Vu que les systèmes sont déjà très complexes, ici, dans quelle mesure serait-il difficile de faire ce que l'Estonie a fait?

● (1030)

Mme Liia Hänni: Selon moi, je crois qu'il a parfois été plus facile pour nous de bâtir le système en considérant la technologie comme un facteur habilitant. Dans de nombreux gouvernements ou de nombreuses démocraties, les gouvernements fonctionnent déjà très bien, alors il n'y a pas de pression pour modifier les processus étatiques et utiliser les nouvelles technologies, mais je crois que, puisque les choses continueront d'avancer et que les citoyens continueront d'utiliser les technologies, le gouvernement doit par conséquent comprendre qu'il est temps de revoir son fonctionnement.

C'est difficile, parce que vous avez un système qui fonctionne bien, alors pourquoi modifier la structure gouvernementale? Je crois que c'est nécessaire, mais il faut beaucoup de volonté politique, de compréhension et de stratégies pour cerner de nouveaux objectifs quant à la façon dont les pays doivent entrer dans le XXI^{e} siècle. C'est en fait du travail très intéressant pour les politiciens de la planète, soit comprendre ces occasions d'obtenir un important consensus national au sujet de l'orientation que le pays veut prendre. C'est la raison pour laquelle je vous félicite. Vous avez cette occasion maintenant.

M. Raul Rikk: Si vous me permettez d'ajouter quelque chose, le processus est encore en cours. J'ai affiché une diapositive qui montre les principaux règlements au sein de l'Union européenne. La même chose qui s'est produite en Estonie se produit maintenant au sein des États de l'Union européenne. La première directive, la réglementation de l'Union européenne sur les données, porte justement sur l'identité numérique et la prestation de services numériques dignes de confiance. La deuxième directive concerne la façon de gérer les incidents. La troisième concerne la protection des données.

Maintenant, l'Union européenne veut adopter la même logique à l'échelle de l'Europe. Au cours des cinq à dix dernières années, l'Union européenne a fait beaucoup d'efforts pour présenter ces règlements et directives et les faire approuver. Ce sera donc maintenant encore plus grand.

Mme Anita Vandenbeld: Pour ce qui est de la motivation à le faire, je crois que des économies de 2 % du PIB constituent une très bonne motivation.

Je vais revenir à la question de la confiance, parce que, bien sûr, nous sommes dans un environnement très différent aujourd'hui que nous l'étions dans les années 1990 et les années 2000 en ce qui a trait au niveau de confiance des citoyens à l'égard des données numériques et aussi, du gouvernement.

Madame Hänni, pouvez-vous nous parler du niveau de confiance à l'égard du gouvernement lorsque vous avez commencé le processus, par opposition, par exemple, à la crainte suscitée lorsqu'il y a communication de renseignements entre des ministères? Je sais qu'il y a eu certaines préoccupations soulevées au Canada quant au fait que certains renseignements soient communiqués aux services de sécurité ou que des renseignements sur la santé ou des renseignements de nature fiscale soient communiqués à d'autres ministères.

De quelle façon vous protégez-vous contre cela? Selon vous, quel était le niveau de confiance des citoyens à l'égard du gouvernement de façon générale, et d'Internet, et en quoi la situation est-elle peut-être différente aujourd'hui? Et de quelle façon peut-on surmonter ce défi?

Mme Liia Hänni: Je crois que, essentiellement, vous demandez de quelle façon on peut créer la confiance.

Tout dépend de la situation dans votre pays. En Estonie, venant d'un système totalitaire où Big Brother nous observait tout le temps, et notre propre gouvernement, il s'agissait d'une situation très différente et nous ne nous sommes même pas vraiment demandé si notre propre gouvernement allait faire un mauvais usage de nos données. Le problème de l'absence de confiance a été très criant en Estonie, d'après ce que j'ai compris, mais les gens doivent tout de même comprendre de quelle façon un système fonctionne. Lorsqu'on a une telle préoccupation, le gouvernement doit pouvoir expliquer les rouages de l'échange de données et la façon dont les données des citoyens sont protégées. Il y a beaucoup de travail à faire là, et c'est quelque chose de plus en plus nécessaire.

Cependant, encore une fois, les documents papier sont beaucoup moins sécuritaires que les renseignements numériques.

● (1035)

Mme Anita Vandenbeld: J'ai une autre question rapide. C'est au sujet de l'âge. À quel âge commencez-vous à recueillir des données? À la naissance? Est-ce lorsque les gens obtiennent leurs premiers permis de conduire? À quel âge est-ce que les citoyens eux-mêmes peuvent avoir accès à leurs données et peuvent les contrôler?

Mme Liia Hänni: En fait, la première donnée numérique qui apparaît dans notre système, c'est lorsqu'un bébé naît. Déjà là, comme je l'ai dit, il s'agit d'un citoyen estonien numérique possédant un code d'identification personnelle, même une carte d'identité personnelle, parce qu'elle peut être utilisée pour les déplacements. Les parents, bien sûr, sont responsables des données de leurs bébés et ils peuvent aussi avoir accès à ces données — par exemple, les données médicales —, mais nous n'avons pas le temps de parler des dossiers médicaux, des systèmes médicaux que nous avons mis en place.

Oui, la collecte de données commence à la naissance, en fait, mais, encore une fois, le gouvernement peut seulement recueillir des données lorsqu'il a le pouvoir légal de demander de telles données. C'est très important de le comprendre. Ce n'est pas aux différents organismes gouvernementaux de décider de me demander des données s'il n'y a pas de motif légal de le faire. Ces genres d'autorisations d'utilisation de données accordées aux différents organismes sont fondées dans la loi. Lorsque les fonctionnaires veulent accéder au système, ils doivent avoir ce pouvoir...

Le président: Je suis désolé, madame Hänni, mais nous avons une dernière question et il reste seulement environ deux minutes.

Je suis désolé, madame Murray. Il nous reste environ quatre minutes ou moins.

Mme Joyce Murray (Vancouver Quadra, Lib.): Merci beaucoup. Je tiens tout simplement à vous remercier du leadership de votre pays dans le dossier du gouvernement numérique. J'ai eu la chance de passer du temps avec Siim Sikkut, votre DPI, à Wellington, pour la signature de la charte du groupe numérique 7. Il est évident que l'Estonie est un chef de file à l'échelle internationale, alors je vous félicite.

Je veux poser une question sur les fonctions de chien de garde. Si quelqu'un a une plainte liée à une violation de la vie privée ou une violation perçue des données personnelles, y a-t-il un chien de garde?

Dans notre pays, nous avons un commissaire qui s'occupe de la protection des renseignements personnels. Nous avons aussi un commissaire dont c'est le travail de traiter les plaintes et de mener des enquêtes. Ils ont des pouvoirs de rendre des ordonnances relativement à l'accès aux renseignements gouvernementaux par les citoyens. J'aimerais connaître la structure de conformité et de surveillance de l'Estonie. Plus précisément, j'aimerais savoir si la surveillance de la protection des renseignements personnels est associée à la surveillance de l'accès à l'information, comme c'est le cas en Nouvelle-Zélande et dans les pays des nombreux autres dirigeants à qui j'ai parlé à Wellington. Nous avons quant à nous séparé ces fonctions, et j'aimerais connaître l'approche de l'Estonie.

Le président: Merci, madame Murray.

Je suis désolé, madame Hänni et monsieur Rikk, mais pouvons-nous obtenir une réponse écrite à la question de Mme Murray? Pouvez-vous répondre de cette façon? Nous n'avons plus de temps, malheureusement.

Je tiens à vous remercier à nouveau d'avoir témoigné pour nous au Canada. Je vous remercie du temps que vous nous avez accordé et de toute votre patience lorsque nous avons dû régler des difficultés techniques. Je vous remercie beaucoup.

Merci de votre leadership en matière de gouvernance numérique.

Nous allons suspendre les travaux et poursuivre la séance à huis clos pour traiter des affaires du Comité.

[*La séance se poursuit à huis clos.*]