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 097 • 1re SESSION • 42e LÉGISLATURE

TÉMOIGNAGES

Le mardi 27 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 mardi 27 mars 2018

● (0845)

[*Traduction*]

Le président (M. Bob Zimmer (Prince George—Peace River—Northern Rockies, PCC)): Je déclare ouverte la séance nº 97 du Comité permanent de l'accès à l'information, de la protection des renseignements personnels et de l'éthique. Conformément à l'alinéa 108(3)h)(vii) du Règlement, nous étudions la protection des données personnelles dans les services gouvernementaux numériques.

Nous accueillons aujourd'hui Jerry Fishenden, technologue et conseiller du gouvernement, à titre personnel.

Allez-y, monsieur Angus.

M. Charlie Angus (Timmins—Baie James, NPD): Je sais que nous discuterons plus tard de la liste des témoins pour l'étude du scandale grandissant au sujet de Facebook. Je suis préoccupé et je tiens à ce que cela figure dans le compte rendu pour que mes collègues y réfléchissent. La question qui se pose en ce moment au Royaume-Uni, de savoir si la plateforme Facebook a été utilisée illégalement pour saboter le vote sur le Brexit et peut-être changer le résultat de ce vote, a potentiellement un lien direct avec le Canada, Jeff Silvester et le travail effectué par l'AIQ. Je crois comprendre que M. Silvester, en raison des limites de compétence, refuse de témoigner devant le comité britannique.

Toutefois, il serait tout à fait conforme au mandat de notre comité d'inviter M. Silvester à témoigner, étant donnée la capacité des exploitants tiers d'utiliser à mauvais escient des données personnelles et de potentiellement subvertir le vote en faveur du Brexit. À cette fin, si nous acceptons de le convoquer à venir témoigner, ce que nous pourrions faire en l'assignant à témoigner au besoin, nous devrions informer le comité britannique de nos travaux. Ainsi, si ce comité a des questions sur la façon dont le référendum a été subverti par cette mauvaise utilisation de la plateforme Facebook, il pourra également nous fournir des notes d'information, afin que nous puissions faire ce travail.

Les répercussions possibles sur le processus démocratique sont beaucoup plus vastes que tout ce que nous avons étudié jusqu'ici. Il y a urgence et j'invite mes collègues à dire que cela vaudrait la peine à ce stade que nous communiquions avec le comité britannique.

Le président: Monsieur Angus, présentez-vous une motion à cet effet ou demandez-vous simplement au président qu'il examine cette possibilité?

M. Charlie Angus: Nous pouvons nous y prendre de plusieurs façons. Je pourrais présenter une motion maintenant. Nous pourrions le faire à huis clos, mais nous devons nous informer de la gravité de la situation, parce que les États-Unis sont en train d'examiner la question. Le Royaume-Uni examine la question et deux des principaux acteurs de cette affaire sont Canadiens. Nous devrions admettre la gravité de la situation et indiquer clairement que nous allons nous y attaquer.

Je sais qu'il y a un certain nombre de témoins dont nous allons parler et je ne veux pas réduire le temps de parole du témoin d'aujourd'hui, mais dans le cas de M. Silvester, nous devrions affirmer qu'il va certainement comparaître devant notre comité.

Le président: Voulez-vous ouvrir la discussion maintenant ou voulez-vous en parler d'abord?

M. Charlie Angus: Je vais céder la parole à M. Erskine-Smith et voir ce qu'il en pense.

M. Nathaniel Erskine-Smith (Beaches—East York, Lib.): Je suis tout à fait ouvert à cette conversation, mais nous devrions en discuter plus tard, après l'exposé de notre témoin. De toute évidence, les analystes ont préparé une note d'information et cela n'en fait pas partie.

J'ai écouté avec intérêt le témoignage de Chris Wylie devant le comité britannique ce matin et je suis donc ouvert à tous les témoins potentiels et au débat sur ce sujet. Nous allons nous en occuper, si j'ai bien compris, après avoir entendu ce témoin, et nous allons nous en occuper comme nous le faisons habituellement, c'est-à-dire après les travaux du Comité. Ayons cette discussion à ce moment-là.

Le président: J'ai également suivi avec intérêt les témoignages de ce matin, nous y reviendrons donc après le témoignage d'aujourd'hui.

Allez-y, monsieur Fishenden.

M. Jerry Fishenden (technologue et conseiller gouvernemental, à titre personnel): Bonjour. Je vous remercie de me donner l'occasion de témoigner. Je le fais à titre personnel, comme vous l'avez mentionné.

Les gouvernements et les entreprises ont absolument besoin de la confiance des consommateurs et des citoyens s'ils veulent utiliser la technologie dans l'intérêt de tous. Pourtant, il arrive trop souvent que des données personnelles soient prélevées et mal employées, soit intentionnellement, soit par suite de l'application de piètres mesures de sécurité et de protection de la vie privée. À titre d'exemple, il suffit de citer les révélations concernant Facebook et Cambridge Analytica.

Nous devons améliorer le niveau général de compréhension au sujet des données et de l'informatique. Tout aussi claire est la nécessité de mieux comprendre les différences importantes qui existent entre les données publiques, ouvertes et les données privées, personnelles. Il nous faut, en particulier, faire en sorte que les données délicates, qui concernent tout le monde, des enfants vulnérables aux agents de police d'infiltration, soient mieux protégées.

Une bonne partie des données du gouvernement sont souvent de mauvaise qualité, étant donné que beaucoup de gens ne traitent qu'occasionnellement avec le gouvernement central. Ces données sont reproduites à de nombreux endroits. Le gouvernement n'a généralement pas d'architectures de données bien conçues. Il lui faut mieux structurer et comprendre son utilisation des données et cesser de croire que le partage des données est un moyen de remédier à une mauvaise conception.

En informatique, nous disposons, d'ores et déjà, de meilleures approches: la preuve à connaissance nulle; l'utilisation des interfaces; le chiffrement; l'authentification et l'autorisation; la confirmation des attributs ou des affirmations. Ainsi, la preuve à connaissance nulle permet à une partie de prouver à une autre partie qu'un énoncé donné est vrai, sans lui transmettre de détails autres que le fait que cet énoncé est vrai: par exemple, dire que j'ai plus de 21 ans ou que j'ai droit à des prestations d'aide sociale.

De telles techniques informatiques doivent être intégrées dans la conception des systèmes. Sinon, plus l'habitude du partage des données, typique de l'ère du papier, persistera à une époque où les systèmes informatiques fonctionnent à une échelle et à une cadence jamais vues auparavant, plus la sécurité, la protection de la vie privée et la confiance se détérioreront vite, et plus les cas de fraude se multiplieront. Les souffrances humaines et les torts financiers causés par la mauvaise utilisation des données ne feront que s'accentuer à moins que les gouvernements n'adoptent des moyens de protection juridiques et techniques plus solides.

Le Royaume-Uni s'est particulièrement inspiré de l'Estonie pour en apprendre davantage à ce sujet. Ce pays applique un ensemble de principes valables, principalement en axant toute son organisation sur le citoyen, au point que ce dernier peut voir quel fonctionnaire accède aux données le concernant. La transparence est essentielle pour permettre de gagner et de maintenir la confiance du public.

En 2011, le député Francis Maude, alors ministre au Royaume-Uni, a mis sur pied le groupe consultatif de la vie privée et des consommateurs. Le groupe comprenait des universitaires, des défenseurs de la sécurité et de la protection de la vie privée et des représentants de groupes de consommateurs. Sa mission consistait à faire en sorte que les programmes du gouvernement prennent en compte le droit des citoyens à la protection de leurs renseignements personnels ainsi que la confiance du public, de la planification initiale des politiques à la mise en oeuvre de ces dernières, en passant par la définition des besoins.

Le groupe a bien fonctionné tant qu'il a eu l'appui direct d'un ministre fort comme Francis Maude, mais, après son départ, des fonctionnaires ont cessé de répondre au groupe ou de participer à ses réunions. Je recommanderais de créer un groupe d'experts semblable, mais d'exiger qu'il rende directement compte au Parlement, peut-être par l'intermédiaire d'un comité comme le vôtre, de manière à ce qu'il ne puisse être marginalisé ou ignoré.

Le code de pratique en technologie du Service du numérique au Royaume-Uni, qui établit un jeu de critères pour aider le gouvernement à concevoir, à construire et à acheter de meilleures technologies, met particulièrement l'accent sur la vie privée. Il précise explicitement que les citoyens doivent avoir accès aux données personnelles les concernant et exercer un contrôle sur elles. Le code établit encore comme principe que la protection de la vie privée doit faire partie intégrante de toute technologie.

La prévention des cyberattaques et la protection des données constituent un défi constant, qu'il s'agisse d'attaques venant de l'extérieur ou d'un acte malveillant d'un intervenant interne, qu'il s'agisse d'un fonctionnaire ayant accédé à des données ou les ayant utilisées de façon inappropriée ou d'un développeur de logiciel qui aurait inséré un code indésirable qu'il pourrait exploiter plus tard. Le Royaume-Uni bénéficie de l'aide et des conseils des experts du National Cyber Security Centre, qui fait partie du Government Communications Headquarters.

Je m'inquiète toutefois du caractère insuffisant des mesures de protection de la vie privée prises par les bureaux d'études de conception et d'ingénierie de sécurité.

● (0850)

De nombreux ministères et organismes du gouvernement ont mis sur pied leurs propres programmes de conception en faisant appel à des développeurs Web, dont bon nombre n'ont ni la formation ni l'expérience voulues pour composer des codes sécurisés. Il faut envisager d'imposer des normes minimales pour garantir la qualité technique des logiciels, par exemple des normes ISO, l' application des principes du Consortium for IT Software Quality, et les conseils d'experts spécialisés comme ceux proposés par le National Computer Security Council.

Au niveau de l'infrastructure, on applique des pratiques exemplaires pour protéger les données actives et inactives. Par ailleurs, il y a un contrôle et une vérification rigoureux de l'accès aux systèmes les plus délicats, notamment en exerçant sur eux une surveillance protectrice.

Une compréhension insuffisante de la technologie, la bonne comme la mauvaise, aux échelons les plus élevés, risque d'engendrer des lacunes dans les politiques et aussi des écarts entre l'intention, les résultats et la législation. Parfois, des lois existantes peuvent empêcher d'améliorer avantageusement les services et leurs résultats; il importe donc d'avoir un processus en place qui mette en lumière les aspects des lois qu'il faut simplifier ou mettre à jour.

Certains responsables politiques et certains fonctionnaires ont naïvement tendance à supposer que la technologie peut résoudre magiquement des problèmes stratégiques ou socioéconomiques complexes. Il faut remettre en question la notion selon laquelle la technologie peut servir à régler tous les problèmes. La discussion ne doit jamais se limiter aux sites Web et aux services en ligne, mais elle doit aussi porter sur la façon dont une meilleure infrastructure numérique aide ceux qui ont encore besoin de services assurés en personne et ceux qui n'utilisent pas la technologie ou qui n'y ont pas accès.

Le gouvernement doit donner l'exemple en matière de consentement en ce qui concerne l'utilisation sécurisée des données et l'établissement des principes à appliquer pour un emploi éthique des données et des logiciels qui servent à les acquérir, les traiter et les utiliser.

Le consentement des utilisateurs est l'une des principales questions sur lesquelles le gouvernement devrait jouer un rôle de premier plan, c'est-à-dire la mobilisation et l'éducation des utilisateurs pour assurer leur participation et leur compréhension consensuelles, y compris pour les données qu'ils révèlent, ce qu'ils font de ces données et comment ils peuvent donner ou annuler leur consentement.

Un autre rôle clé du gouvernement est de veiller à ce que les lois soient à la hauteur des besoins ou de repérer les mises à jour nécessaires en fonction de l'évolution de la technologie

Le gouvernement peut également jouer un rôle dans les questions économiques, comprendre les effets qu'une meilleure utilisation des données et des techniques comme l'intelligence artificielle et l'apprentissage automatique auront sans doute au niveau micro et macroéconomique, notamment sur la configuration future possible des services publics, à mesure que l'Internet des objets et les capteurs de l'état de santé, par exemple, seront plus répandus.

Il y a aussi les problèmes d'accès et de contrôle. Il faut établir un cadre de confiance qui couvrira l'anonymisation, la pseudonymisation et de rigoureux modes de confirmation de l'identité.

J'ai déjà parlé de la qualité des données. Il s'agit de veiller à ce que l'exactitude et la véracité des données soient suffisantes pour garantir la cohérence des décisions fondées sur celles-ci. Avant de construire des analyses et de s'adonner à l'apprentissage automatique à l'aide de données dont on ne connaît pas la qualité, il faudrait procurer aux utilisateurs un accès à leurs propres données pour qu'ils confirment l'exactitude de leur dossier.

La dépersonnalisation et de l'anonymat des données sont des problèmes connus qui se posent déjà lorsqu'il s'agit d'anonymiser correctement les données personnelles. Cela devient un enjeu de plus en plus important et complexe. La dépersonnalisation n'est pas la même chose que l'anonymisation. Il faut approfondir les recherches pour clarifier cette différence

En ce qui concerne l'accès aux données, nous devons veiller à ce que des mécanismes de contrôle appropriés soient en place pour les données publiques, privées ou personnelles auxquelles de tels systèmes accèdent. Avec notamment l'application de mesures appropriées de protection de la sécurité et de la vie privée, de vérification, de responsabilisation et de surveillance protectrice.

En ce qui concerne la véracité et l'intégrité des données, comment pouvons-nous savoir que les données utilisées par de tels systèmes sont fiables? Comment savons-nous que les systèmes ont fourni toutes les données quand nous essayons de les réglementer ou de veiller à ce qu'ils soient conformes aux lois sur la non-discrimination, par exemple?

En ce qui concerne le champ d'application des lois vis-à-vis des codes, les codes et les données existent de plus en plus dans le nuage ou dans des environnements sans serveur, dans des systèmes disséminés partout dans le monde. Il faut savoir précisément comment ils répondent aux normes exigées — par exemple sans avoir des comportements tendancieux, illicites ou discriminatoires, ou sans être compromis par des acteurs hostiles.

Enfin, en ce qui concerne la résilience, comme de nombreux services dépendent de plus en plus de cette nouvelle génération de systèmes interconnectés, la résistance potentielle aux pannes accidentelles ou malicieuses est un enjeu important. D'autres recherches sont nécessaires sur les interactions et les vulnérabilités éventuelles et sur les risques inhérents à ces systèmes de systèmes en devenir.

Si les meilleurs cadres juridiques, éthiques et axés sur la confiance ne sont pas mis en place, les modes mal conçus d'acquisition et d'utilisation des données personnelles seront discriminatoires, faux, inexacts ou tendancieux. Ils se caractériseront par l'irresponsabilité et la manipulation, créeront d'importants problèmes au chapitre de la sécurité, de la protection de la vie privée et des régimes juridiques et ils fragiliseront la confiance.

● (0855)

Cependant, s'ils sont bien appliqués, ils aideront à améliorer l'élaboration des politiques, les soins de santé, l'éducation et les transports, entre autres, grâce à des systèmes adaptés et plus efficaces.

Il faut des normes cohérentes de sécurité, de protection de la vie privée et de génie logiciel en même temps que de la transparence. Pour qu'une initiative numérique ou cybergouvernementale soit fructueuse, les responsables doivent d'abord décider ce qu'ils veulent accomplir en passant au numérique. S'agit-il simplement d'automatiser les services actuels? Ou s'agit-il d'une optimisation, d'une restructuration ou d'une transformation? S'agit-il d'affecter des ressources en première ligne et, pour cela, de réduire le coût des opérations internes en aidant à les simplifier? Il importe de connaître exactement les résultats et les bienfaits souhaités, au lieu de supposer tout simplement que c'est quelque chose que nous devons faire à l'ère numérique.

Le gouvernement doit jouer un rôle important et positif en montrant comment nous pouvons profiter des avantages de cette ère numérique au lieu d'en subir les inconvénients. Plutôt que de se laisser guider simplement par les pires paramètres appliqués par le secteur privé en utilisant les données à mauvais escient et en s'en servant de façon abusive sans le consentement éclairé des utilisateurs, les gouvernements doivent viser à élever les normes. Ils ont une chance de prendre l'initiative.

Je me ferai un plaisir de vous fournir des liens et des références plus détaillés après la séance d'aujourd'hui, si cela vous est utile. Merci d'avoir pris le temps de m'écouter.

● (0900)

Le président: Merci encore, monsieur Fishenden.

Nous allons commencer par M. Nathaniel Erskine-Smith. Vous avez sept minutes.

M. Nathaniel Erskine-Smith: Merci beaucoup.

Dans le cadre de cette étude, nous examinons comment le gouvernement numérique peut améliorer les services offerts aux Canadiens tout en protégeant leur vie privée et leur sécurité. Avez-vous un cas idéal, un exemple que nous pourrions citer et dire: « Voici une initiative qui a fonctionné ?»

M. Jerry Fishenden: Il y a eu plusieurs initiatives dans le cadre desquelles la protection de la vie privée a été au coeur du programme. Je crois que certains programmes ont connu des difficultés. Je pense notamment au programme GOV.UK Verify, qui examine l'identité. Il est fondé sur un ensemble très solide de principes de protection de la vie privée et il a été conçu dès l'origine pour assurer le respect de ces principes et pour tenir compte des lois à venir, comme le règlement général sur la protection des données de l'Union européenne. Cependant, je pense que pour d'autres raisons, ce programme a eu des difficultés à obtenir les résultats escomptés.

J'ai également collaboré à d'autres types de projets, notamment à certains systèmes nationaux de police, qui sont généralement très bien conçus pour protéger les données des citoyens concernés et pour lesquels il y a une surveillance de protection. Malheureusement, il y a eu un ou deux cas qui ont prouvé l'intérêt de la surveillance protectrice, lorsque des agents de police ont fini par être repérés, parce qu'ils avaient abusé de la confiance en ayant accès à ces systèmes. Je pense que nous devons chercher des moyens d'assurer une surveillance plus proactive des systèmes afin qu'en cas d'abus potentiels de ce type de la part d'un initié ou évidemment dans le cas d'un acteur extérieur hostile, nous soyons beaucoup plus réactifs face à ces incidents.

M. Nathaniel Erskine-Smith: Pour ce qui est des cas exemplaires, cependant... Dans vos remarques, vous avez dit que le Royaume-Uni se tournait vers l'Estonie. La semaine dernière, des représentants de l'Estonie ont comparu devant nous et nous ont parlé très éloquemment de leur système. Il a amélioré les services. Ils ont réduit les coûts — 2 % du PIB. Aucune identité numérique n'a été usurpée. Est-ce, à votre avis, le modèle à l'échelle internationale?

M. Jerry Fishenden: J'ai beaucoup de respect pour l'approche estonienne et j'ai passé du temps avec les fonctionnaires et les responsables politiques de ce pays.

Pour être franc, je pense que l'une des choses avec lesquelles nous avons eu des difficultés au Royaume-Uni, c'est que l' approche de l'identité utilisée par l'Estonie est manifestement très différente de celle adoptée au Royaume-Uni. C'est le coeur du système. Au Royaume-Uni, nous avons encore des difficultés à adopter un cadre d'identité fiable et uniforme qui permettrait aux citoyens non seulement de prouver facilement qui ils sont lorsqu'ils sont en ligne, mais aussi de prouver qu'un ensemble de données particulier leur appartient, ce qui est une question beaucoup plus complexe. Même si j'ai prouvé mon identité à une tierce partie, lorsque je me présente au service national de santé ou du bureau d'aide sociale du Royaume-Uni et que j'essaie de demander l'accès à un dossier particulier, il faut encore associer mon identité aux données particulières conservées dans différents silos de données à l'échelle du gouvernement et cela s'avère également un défi assez complexe.

M. Nathaniel Erskine-Smith: C'est un point intéressant, parce que lorsque les fonctionnaires estoniens ont comparu devant nous la semaine dernière, mon collègue, M. Baylis, leur a demandé de nous expliquer les éléments de base, le point de départ de la démarche. Ils ont dit que le point de départ devait être l'identification numérique. Ils ont fait remarquer que leur carte d'identité numérique est en soi un dispositif de chiffrement, ce qui explique pourquoi ils n'ont pas eu les problèmes d'usurpation d'identité que nous avons eus ici en n'ayant pas d'identité numérique.

Vous avez critiqué le programme d'assurance numérique actuel du Royaume-Uni. Est-ce ce que l'Estonie a fait...? La question fondamentale est la suivante: pourquoi ne pas faire exactement ce que l'Estonie a fait?

M. Jerry Fishenden: C'est une bonne question, qui se prolonge dans le domaine politique. Le programme actuel d'assurance de l'identité Verify a été créé après l'abolition du programme des cartes d'identité du Royaume-Uni par le nouveau gouvernement de 2010. C'était une promesse politique du gouvernement de coalition réunissant les libéraux-démocrates et les conservateurs. Ils étaient très désireux de trouver une méthode permettant d'obtenir un résultat semblable, mais qui n'exige pas que tous les citoyens du Royaume-Uni doivent inscrire leurs données biométriques dans un registre national d'identité. C'était un effort pour trouver une solution intermédiaire.

Il y a aussi, en partie, des changements comme le système bancaire ouvert, mis en oeuvre récemment au Royaume-Uni, qui permet de prouver qui vous êtes en utilisant votre banque pour confirmer votre identité en ligne et confirmer par l'entremise d'une tierce partie que vous êtes bien qui vous dites être. Je pense qu'on veut réfléchir en ce moment à ce que le gouvernement voulait réaliser à l'origine, c'est-à-dire un marché de fournisseurs d'identité dignes de confiance travaillant dans un cadre auquel le gouvernement faisait confiance et qu'il pourrait réglementer au besoin, et la question est de savoir si cela peut se faire grâce aux changements qui se produisent sur le marché de toute façon.

Ce qui me semble manquer est le lien entre une identité avérée et les divers silos de données qui me concernent ou qui m'appartiennent dans les différents ministères. Il faudrait discuter davantage du processus qui va lier mon identité à ces différents ensembles de données de façon à ce que les gens puissent...

● (0905)

M. Nathaniel Erskine-Smith: Vous avez dit, justement, que c'est la politique qui, en quelque sorte, y fait obstacle. À supposer que nous supprimions la politique de l'équation, la meilleure solution serait-elle d'adopter ce que l'Estonie a fait avec l'identification numérique dans son dispositif de chiffrement ou diriez-vous qu'il y a des façons d'améliorer l'expérience estonienne?

M. Jerry Fishenden: Je pense qu'on pourrait démarrer en suivant une voie très semblable à celle de l'Estonie. De nos jours, la plupart des gens emportent avec eux des téléphones ou des appareils mobiles. Ces appareils mobiles pourraient servir de principal moyen de prouver l'identité. C'est comme cela que je procède pour bon nombre de mes services commerciaux en ligne. J'ai un système d'authentification ou de vérification à deux critères, et, quand j'essaie de me connecter en ligne, je reçois, selon le cas, un code temporaire que je peux lire à partir de mon téléphone, ou un message texte, ce qui est évidemment moins sécuritaire. Je pense que le gouvernement pourrait profiter des améliorations technologiques qui ont été apportées depuis que les Estoniens ont élaboré leur modèle pour trouver une solution axée sur les appareils mobiles et plus susceptible d'être fiable.

Je pense que, au Royaume-Uni, le problème était, entre autres, que le Home Office était perçu comme l'arbitre du registre national d'identité et qu'on avait l'impression que les gens devraient stocker toutes leurs données biométriques et personnelles auprès d'un seul ministère. Je pense qu'il y aurait maintenant des moyens plus efficaces de relier une identité avérée aux différents silos ou dépôts de données pour que je puisse prouver qui je suis au Service national de la santé et confirmer le lien avec mes dossiers de santé sans nécessairement révéler ce lien au ministère de l'Impôt ou au ministère du Bien-être social, s'il ne me convient pas de le faire ou si aucune réglementation ne m'y oblige.

Le président: Merci, monsieur Erskine-Smith.

C'est à vous, monsieur Gourde.

[*Français*]

M. Jacques Gourde (Lévis—Lotbinière, PCC): Je vous remercie, monsieur le président.

Je vais revenir sur les données numériques des citoyens canadiens, et peut-être celles de citoyens d'autres pays aussi, qui sont acheminées à différents ministères où les gens travaillent en vase clos.

En 12 ans, depuis que je suis député, je me suis aperçu qu'une partie des problèmes de mes concitoyens, quand ils viennent me demander de l'aide, découle du fait qu'il y a des données erronées, des données qui ne sont pas les mêmes d'un ministère à l'autre. Cela leur cause des difficultés. Nous devons alors faire une recherche avec eux pour les aider à rétablir l'exactitude des données. Par exemple, c'est souvent une adresse qui diffère d'un ministère à l'autre, tout simplement. Cela fait que des citoyens perdent des droits ou des services, entre autres.

Pour améliorer le fonctionnement du travail en vase clos, ne pourrait-on pas créer un fichier numérisé personnel pour chaque individu? Chacun aurait droit à son fichier, qui lui appartiendrait, et il pourrait le corriger lui-même pour que les données soient réelles, véridiques et en temps réel? Ce pourrait être la responsabilité de l'individu de voir à ce que son fichier soit toujours tenu à jour.

[*Traduction*]

M. Jerry Fishenden: Vous brossez un tableau qui m'est familier. Cela ressemble beaucoup au modèle du Royaume-Uni, où les données sont conservées à plusieurs endroits, souvent avec des renseignements contradictoires.

Je suis convaincu que le citoyen doit absolument avoir accès à ses données et pouvoir les contrôler précisément pour cette raison. C'est le citoyen qui doit être l'arbitre ultime de ses propres données, évidemment sous réserve d'une certaine validation par le gouvernement s'il y a lieu. Qu'il puisse gérer ses propres dossiers serait un bon moyen de le faire, comme on le fait avec les organisations commerciales lorsque nous ouvrons une session et que nous mettons à jour les détails de notre carte de crédit ou nos adresses.

Une partie du Royaume-Uni a commencé à le faire. Nous avons maintenant un portail fiscal unique. Lorsque je me connecte, j'ai accès non seulement à ma situation fiscale actuelle, mais aussi ma situation de retraité de l'État, même si ces données proviennent de ministères distincts. Cela me permet de voir au même endroit des données provenant de plus d'un silo gouvernemental.

Je ne pense pas que le fait de permettre aux citoyens d'avoir accès à leurs dossiers et de les tenir à jour signifie qu'il faut regrouper toutes les données dans une seule base de données. On craint toujours que, si tout se trouve au même endroit, une atteinte à la protection des données les touche toutes. Les cloisonnements sont utiles si c'est à juste titre et si l'utilisateur, le citoyen, peut quand même gérer ses données par l'entremise d'un seul service en ligne, même si les données mises à jour sont ensuite retournées dans...

Je pense à des domaines comme la santé, où les citoyens sont particulièrement sensibles au fait que leurs dossiers pourraient être mis à la disposition d'autres personnes. Je pense que, d'une certaine façon, le fait de cloisonner délibérément les dossiers de santé peut être une bonne chose, mais on pourrait tout de même permettre au citoyen de mettre à jour les aspects communs de ces dossiers dans les différents organismes gouvernementaux, comme les adresses, par le biais d'un seul portail.

À mon avis, cela revient à la question de l'identité, qui doit vraiment être réglée en premier. Il faut savoir à qui l'on a affaire, puis confirmer qu'il est vraiment celui à qui appartiennent ces différents répertoires de données. Je suis donc tout à fait d'accord pour dire que le citoyen est bien placé pour examiner les données et pour, selon le cas, apporter directement des modifications et des corrections ou pour demander au ministère compétent de les apporter.

● (0910)

[*Français*]

M. Jacques Gourde: Un fichier central permettrait sans doute aux citoyens d'être informés du fait que tel ministère ou tel organisme utilise leurs données si ces derniers en demandaient l'autorisation en vue de la prestation de services. Par exemple, l'Agence du revenu du Canada pourrait demander l'autorisation d'accéder au fichier numérique central d'une personne pour régler tel ou tel problème. Actuellement, les citoyens canadiens ne savent pas quels ministères consultent leurs données numériques existantes.

Je crois que ces données appartiennent aux individus et que ceux-ci doivent être au courant du fait qu'un organisme fait des recherches à leur sujet.

Pensez-vous qu'il serait légitime que les individus en question demandent d'être tenus au courant du fait qu'un ministère examine leurs données numériques?

[*Traduction*]

M. Jerry Fishenden: Oui, je pense que le principe est très valable. Évidemment, il y a des cas où l'État a besoin de faire des enquêtes d'arrière-plan dont il ne conviendrait pas d'avertir le citoyen, par exemple en cas de fraude ou de crime, mais je pense que c'est un principe général valable.

C'est une des raisons pour lesquelles j'aime bien le système estonien. Les citoyens estoniens peuvent voir quels ministères et fonctionnaires ont consulté leurs dossiers et, s'ils estiment que cela n'avait pas de raison valable, ils peuvent demander des explications. Je suis convaincu que ce serait une très bonne façon de procéder.

[*Français*]

M. Jacques Gourde: Sur le plan de la santé, c'est vraiment très intéressant.

Quand on se rend à l'hôpital, il y a sur place un dossier nous concernant. Ce dossier est partagé ou il ne l'est pas. Au cours de notre vie, si on change de médecin, il arrive malheureusement que les dossiers ne soient pas entièrement transmis, ou alors que les informations qu'ils contiennent soient insuffisantes.

Les données numériques, sur le plan de la santé, devraient être contenues dans un dossier qui nous suivrait toute notre vie. Ce serait plus pratique et sécuritaire pour les individus. Qu'en pensez-vous?

● (0915)

[*Traduction*]

M. Jerry Fishenden: L'idéal serait d'avoir un dossier de santé composite.

Je suis également très conscient, compte tenu de l'utilisation croissante d'appareils portables, que nos renseignements sur la santé couvrent désormais un champ beaucoup plus vaste qu'auparavant. Par exemple, je porte un appareil qui mesure ma fréquence cardiaque et mon entraînement. Il serait bon que tout cela soit regroupé en un seul endroit, pour que, lorsque je vais voir mon médecin, il puisse être informé non seulement de mon dossier médical, mais aussi de mon mode de vie.

Je pense qu'il faut que le citoyen soit le gardien de ses données ou, du moins, qu'il y ait accès et les contrôle pour décider ce qu'il est disposé à communiquer à différents fonctionnaires. Je ne vois pas d'inconvénient à communiquer toutes les données médicales de mes appareils portables à mon médecin. Ainsi, quand je vais le voir, il peut vérifier si je dis la vérité sur mon rythme d'exercice ou, au moins, se faire une idée de mon mode de vie pour m'offrir de meilleurs soins.

Je pense que c'est un élément important qu'on oublie parfois, surtout dans le système que nous avons au Royaume-Uni, à savoir que de plus en plus de données sur la santé ne sont plus conservées exclusivement dans le système de soins de santé. Comme consommateurs et comme citoyens, nous allons produire beaucoup de renseignements médicaux utiles qui doivent aussi être versés dans ces dossiers.

Je suis fondamentalement d'accord pour dire qu'il serait bon d'avoir un endroit très fiable où nous pourrions stocker à la fois les données des services médicaux et nos propres données médicales, afin qu'il y ait un dépôt unique des données sur la santé qui permettrait aux professionnels de la santé de nous fournir les meilleurs soins possible.

Le président: Merci.

C'est à vous, monsieur Angus, vous avez sept minutes.

M. Charlie Angus: Merci. Cette discussion est passionnante.

J'ai appris une chose durant mes nombreuses années au Parlement, c'est que je suis devenu très méfiant à l'égard d'un gouvernement qui dit qu'il va trouver une excellente nouvelle application qui va rendre tout facile et bon marché, parce que, lorsqu'il est question de protection de la vie privée, cela ne semble pas faire partie de la culture opérationnelle.

Par exemple, la semaine dernière, j'ai appris que le gouvernement avait compromis 250 000 dossiers personnels de citoyens, dont leur dossier fiscal, leur dossier de santé, en fait toutes sortes d'autres dossiers. Le nombre de cas avait baissé depuis 2013, époque où un million de dossiers personnels avaient été compromis, dont 583 000 dossiers financiers d'étudiants ayant contracté un prêt.

À chaque fois, année après année, le taux de signalement des fonctionnaires au commissaire à la protection de la vie privée... Au Canada, s'il y a une atteinte grave à la vie privée, on doit la signaler au commissaire à la protection de la vie privée, qui fait enquête pour déterminer s'il y a eu menace pour les données personnelles. Le taux de signalement du gouvernement est de 4 %. Autrement dit, lorsqu'il s'agit de déterminer ce qui est prioritaire, on se soucie toujours d'abord de protéger les arrières du ministre et d'essayer de ne pas attirer l'attention sur lui, au lieu de protéger le principe de la protection de la vie privée.

D'après votre expérience au Royaume-Uni, comment peut-on s'assurer que le gouvernement fait passer la protection de la vie privée avant la protection des ministères et des erreurs? Ces atteintes à la vie privée se produisent année après année, et elles sont très graves.

M. Jerry Fishenden: C'est une bonne question.

Je pense que cela revient, entre autres, à ce qui me préoccupe au sujet de l'ingénierie de la protection des renseignements personnels et de la sécurité. Il serait possible de prévoir un signalement automatique des atteintes d'ordre technique pour qu'elles soient rendues visibles sans interprétation humaine ni ambiguïté dans le processus. J'essaie de trouver des façons polies de le dire.

Je pense aussi qu'il faut se méfier de l'idée que la technologie seule peut fournir la réponse. Cela pourrait certainement aider, notamment à voir où, comme en Estonie, des dossiers ont peut-être été consultés sans raison. On pourrait aussi déterminer où cela se produit peut-être à grande échelle. Par exemple, si quelqu'un, un initié ou un agent externe, a essayé de consulter de multiples dossiers en très peu de temps, il faudrait que cela puisse être repéré très rapidement par un bon système informatique.

Cependant, il semble que la plupart des atteintes à la vie privée révélées au Royaume-Uni concernent souvent des initiés qui ont commis des attaques d'ingénierie sociale. Même dans un système bien conçu, si on fait apparaître des dossiers à l'écran et qu'on utilise des méthodes d'attaque analogiques, par exemple en prenant note des renseignements ou en prenant une photo de l'écran, le système à lui seul ne peut pas repérer ce genre de choses. On peut repérer les tendances comportementales au fil du temps, mais si un fonctionnaire ne le fait qu'une seule fois, ce sera très difficile à savoir.

Il y a aussi un élément dissuasif dans le système actuel, en ce sens que plus les ministères sont honnêtes, plus ils font piètre figure dans les statistiques. On pense qu'ils sont les plus problématiques, alors qu'ils sont peut-être, en fait, les plus honnêtes.

● (0920)

M. Charlie Angus: C'est bien ce qui me préoccupe. Nous pouvons créer le système technologique le plus parfait qui nous vaudra le plus d'éloges, mais cela dépend du facteur humain. Le facteur humain en politique est toujours défini par la politique et les pressions politiques. Dans notre pays, le ministère du Revenu fait l'objet de multiples atteintes à la vie privée, année après année, à cause de la perte de disques durs et de clés USB. Peut-être que, au fur et à mesure que nous nous orientons vers la nuagique, nous ne perdrons pas autant de clés USB remplies de renseignements financiers.

Il s'est produit des cas où des gens ont eu accès aux renseignements de leur ex-conjoint ou de leur conjoint sans raison valable. Ces choses se produiront dans les ministères, je suppose, mais comment instaurer une culture de la responsabilité au sein du gouvernement pour veiller à ce que la protection des renseignements personnels passe avant tout? Sans cette confiance, les citoyens n'ont aucune raison de croire que cette magnifique nouvelle application que nous allons créer va les protéger.

M. Jerry Fishenden: Je suis d'accord. Je pense qu'il y a probablement plusieurs solutions. La première consiste à améliorer la qualité de la formation et de la sensibilisation des fonctionnaires. La deuxième consiste à améliorer la conception de certains systèmes. Par exemple, pourquoi tant d'écrans consultés par les fonctionnaires qui y accèdent révèlent en texte explicite tout ce qui concerne une personne? S'ils ont besoin de savoir si quelqu'un touche une prestation particulière ou s'il a dépassé un certain âge, pourquoi révéler en même temps la date de naissance de la personne ou toutes les prestations qu'elle reçoit? On pourrait simplement avoir un indicateur de confirmation à l'écran, ce qui empêcherait la fuite d'une quantité de données.

Au bout du compte, j'imagine qu'on a besoin de sanctions plus sévères, de sorte que, lorsque ces choses se produisent, les gens soient tenus responsables. On dirait bien que le Canada est dans une situation semblable à celle du Royaume-Uni. Il est extrêmement rare que quelqu'un soit tenu personnellement responsable.

Ce qui est pire parfois, à mon avis, c'est que des amendes sont imposées à des organisations qui font partie du secteur public. Supposons qu'une fiducie de soins de santé ait fait l'objet d'une atteinte à la vie privée, elle pourrait se voir imposer une amende de plusieurs millions de livres. Cela me semble être une double punition pour les innocents, parce que cette amende aura une incidence directe sur le reste d'entre nous, c'est-à-dire sur les gens qui comptent sur les services médicaux de cette fiducie. En fin de compte, cela évite aussi de chercher à savoir qui était responsable. C'est comme si une mystérieuse entité sans visage était responsable.

De plus, à l'échelle des cadres supérieurs, on attribue rarement les responsabilités à qui de droit, qu'il s'agisse du conseil d'administration ou de l'équipe de direction, autrement dit à des gens qui doivent assumer et dont on peut dire: « Voilà, c'est ici que ça s'arrête, ce sont eux qui sont responsables. » Peut-être que, si l'on attribuait clairement la responsabilité à tel ou tel fonctionnaire, on pourrait s'éloigner d'un système d'amendes au Royaume-Uni et que l'on pourrait chercher à savoir qui est responsable de garantir tous les aspects dont nous parlons ici — en s'assurant que la culture organisationnelle est correcte et que les systèmes sont bien conçus — afin que les gens soient tenus responsables lorsque les choses tournent mal et qu'il les corrigent.

Au bout du compte, s'ils ne réussissent pas à régler tous ces problèmes au cours d'une période convenue, ils devraient être tenus responsables.

M. Charlie Angus: Merci beaucoup.

Le président: Merci, monsieur Angus.

Monsieur Baylis, vous avez sept minutes.

M. Frank Baylis (Pierrefonds—Dollard, Lib.): Bonjour... mais c'est déjà l'après-midi pour vous, monsieur Fishenden.

L'un des points importants que vous avez soulevés, c'est que le fondement du système est le cadre de l'identité. L'Estonie a un numéro à 11 chiffres. Vous avez également dit que, au Royaume-Uni, on a envisagé un programme de cartes d'identité en 2010. J'ai l'impression, d'après ce que vous avez dit, que cela n'a pas fonctionné.

Pouvez-vous nous expliquer ce qu'était le programme des cartes d'identité et pourquoi il n'a pas fonctionné ou ce qui est arrivé à ce programme?

M. Jerry Fishenden: Je tiens à préciser que le programme des cartes d'identité a pris fin en 2010 avec l'arrivée d'un nouveau gouvernement. Il a commencé vers 2005 ou 2006.

C'était, en réalité, un programme en deux parties. Il y avait, d'une part, un registre national de l'identité, qui devait contenir quelque 140 renseignements personnels biographiques et biométriques. Le principe voulait que les citoyens s'inscrivent en fournissant leurs empreintes digitales, leurs empreintes rétiniennes, leurs photos, etc.

La carte serait la concrétisation physique du registre. En fait, les citoyens du Royaume-Uni la porteraient sur eux, et elle pourrait être vérifiée au besoin. Elle permettrait aussi de consulter le registre central et, au besoin, de récupérer les empreintes digitales et autres éléments pour permettre à un agent d'application de la loi ou à toute autre personne habilitée de confirmer que la personne présente était bien celle à qui la carte avait été délivrée.

● (0925)

M. Frank Baylis: Si on n'avait pas mis fin au projet, ç'aurait pu être l'identité de base de la transition vers une économie numérique. Pourquoi a-t-il été aboli?

M. Jerry Fishenden: Pour diverses raisons, dont la question des libertés civiles. On considérait qu'il s'agissait d'une base de données unique sur tous les citoyens du Royaume-Uni, qui est étranger à la culture britannique, excepté durant la Seconde Guerre mondiale; les gens avaient alors une carte d'identité, mais cela s'est terminé après la guerre.

Il y a eu également des problèmes d'ordre technique liés à la conception, et il en a été question en partie dans la discussion que nous avons eue sur la question de savoir s'il faut élaborer une grande base de données où seraient versées toutes ces données confidentielles, avec le risque qu'elles puissent être compromises. Cela entraînerait un problème encore plus grave.

M. Frank Baylis: Cette approche est un peu différente de celle, disons, de l'Estonie, où, d'après ce qu'on a dit, on vous donne un numéro à 11 chiffres. Grâce à ce qu'on appelle les « données de sortie », ce numéro permet de tirer ces renseignements de la base de données, mais les deux ne sont pas liés du tout. Les gens qui ont des renseignements dans cette banque de données ne peuvent pas consulter d'autres bases du gouvernement pour les obtenir. Vous dites que cette carte a rendu les gens nerveux, parce que tout était mis ensemble. Ils se sont beaucoup inquiétés de leurs libertés civiles. Je peux le comprendre. C'est bien cela?

M. Jerry Fishenden: Oui, tout à fait. 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, si vous voulez, logiquement là où il est logique de le faire pour l'État — donc peut-être dans les domaines de la santé, de l'impôt, du bien-être social, de l'éducation, etc. —, les citoyens ont toujours le sentiment que ce sont eux, et non pas l'État, qui exercent un contrôle sur leur identité.

M. Frank Baylis: Au Canada, nous avons ce qu'on appelle un numéro d'assurance sociale, qui est un numéro d'identification unique à neuf chiffres. Tous les citoyens en ont un, mais il est surtout utilisé pour Revenu Canada, qui est notre filet fiscal. Existe-t-il au Royaume-Uni un numéro attribué systématiquement à tous les citoyens?

M. Jerry Fishenden: Nous avons plusieurs numéros. Il y a le numéro d'assurance national, qui est délivré par le ministère du travail et des pensions et qui est utilisé principalement par ce ministère. Il y a les numéros de référence fiscaux, qui sont utilisés par le ministère de l'impôt, du revenu et des douanes de Sa Majesté. Et il y a les numéros des Services nationaux de santé, et la plupart des autres ministères ont leurs propres identificateurs individuels.

Pour revenir à mon premier commentaire, ce n'est pas nécessairement un problème, parce qu'il n'y a aucune raison de ne pas avoir de numéro, comme en Estonie, qui soit superposé aux autres et qui permette de prouver qui on est à chacun de ces différents systèmes d'indexation, si vous voulez, mais sans qu'on puisse nécessairement consulter le dossier d'identité proprement dit.

M. Frank Baylis: Oui, en effet, nous avons chacun notre propre numéro d'identité médicale. Le problème, c'est que c'est provincial. C'est une compétence différente, mais, au niveau fédéral — et c'est le gouvernement fédéral qui vous parle en ce moment —, nous avons le numéro d'assurance sociale à neuf chiffres. Est-ce que ces numéros d'assurance nationale, de référence fiscale...? Je vous pose une question technique sur l'importance de ces numéros. Sont-ils alphanumériques? Ce sont tous des identificateurs uniques, n'est-ce pas?

M. Jerry Fishenden: Oui, ce sont le plus souvent des numéros alphanumériques. Le numéro des services de santé peut être purement numérique, mais les autres sont un mélange alphanumérique. J'essaie de me rappeler. Mon numéro d'assurance national a dix chiffres au total. Ce sont cinq nombres à deux chiffres...

M. Frank Baylis: Vous avez dit également que certaines personnes songent à utiliser la confirmation bancaire. Essentiellement, la confirmation bancaire n'est que votre numéro de compte bancaire.

J'aimerais savoir ce que vous en pensez du point de vue du Royaume-Uni. Vous avez besoin d'un identificateur unique. Vous devez choisir des nombres ou une combinaison alphanumérique. Ce sera lié. L'approche du Royaume-Uni, qui semblait trop intrusive, consiste à tout verser dans une même base de données et à le relier à ce même numéro, de sorte que les gens ont commencé à avoir l'impression qu'on s'attaquait à leurs libertés civiles. C'est très différent de ce qui se passe en Estonie, où l'on dit: « Voici votre numéro. Il peut vous relier à n'importe quel ministère et vous donner accès à n'importe quelles données de ce ministère, mais ces ministères ne peuvent pas l'utiliser pour accéder à vos données et se servir de ce système. » Cela vous appartient en propre, et il y a là une idée très forte: c'est qu'on est propriétaire de ses données, qu'on les contrôle et qu'on peut savoir si elles sont utilisées.

Est-ce que ç'aurait été utile? Je sais que vous avez eu des difficultés au Royaume-Uni. Peut-être pourriez-vous nous en dire davantage. Est-ce que ç'aurait été utile? Est-ce que ce serait la bonne façon de procéder si nous envisageons de faire quelque chose au Canada?

● (0930)

M. Jerry Fishenden: Oui, je pense que cette approche pourrait fonctionner, contrairement à celle du Royaume-Uni. Je pense que cela règle aussi la question de savoir comment trouver des données personnelles dans différents silos et les relier à une identité. C'est vous qui établissez l'identité. Je pourrais me présenter quelque part et prouver qui je suis au moyen d'un passeport ou, peut-être, d'un système de reconnaissance faciale, etc., mais cela ne prouve toujours pas que je suis propriétaire de mon dossier national d'assurance ou de mon dossier médical.

La meilleure solution serait que, la prochaine fois que je verrai mon médecin ou un conseiller, je puisse leur prouver qui je suis et que cela renvoie à cette identité avérée. En peu de temps, je pourrais avoir mon identité contrôlée, si vous voulez, et, par mes actions et ma relation de confiance avec les gens qui délivrent les autres numéros, je pourrais prouver que je suis bien la personne à qui ces autres données se rapportent.

Nous nous retrouvons donc là où il faut si nous voulons permettre aux citoyens d'avoir un meilleur accès à leurs propres données et de les contrôler, quand on parle de l'identité fiable et du lien entre cette identité et ces données potentiellement sensibles.

Le président: Merci, monsieur Baylis.

La parole est à vous, monsieur Aboultaif. Vous avez cinq minutes. Bienvenue à vous.

M. Ziad Aboultaif (Edmonton Manning, PCC): Merci.

Bonjour.

On a beaucoup parlé de l'Estonie. Aucun des pays du G20 ou du G7, à ce qu'il paraît, n'a de système ou de modèle que nous puissions examiner. Je crois savoir que le témoin de l'Estonie a comparu devant le Comité et a dit que, d'après son expérience, il n'y a jamais eu aucune atteinte à la vie privée dans leur système.

Est-il raisonnable, d'après vous, de croire qu'il n'y en ait jamais eu? Ou alors, ils ont été piratés et ne l'ont jamais su. Qu'en pensez-vous?

M. Jerry Fishenden: C'est une question très difficile. C'est dans la nature même de la sécurité informatique et des systèmes que de découvrir seulement des années plus tard qu'il y a eu atteinte à la vie privée.

Compte tenu de la compétence des gens que j'ai rencontrés et de ce que je sais de leur système, ils bénéficient des meilleures garanties informatiques qui soient pour protéger leurs activités. Quant à savoir s'il pourrait arriver qu'il y ait eu un code malveillant ou que des données soient compromises, c'est presque impossible à dire.

Je pense qu'ils ont beaucoup de savoir-faire et qu'ils sont très attentifs à surveiller, dans leur propre environnement, les comportements étranges qui ne sont pas conformes aux normes. C'est une tendance que nous commençons à voir ailleurs, du côté des banques et des compagnies d'assurances qui offrent des transactions en ligne au Royaume-Uni, mais aussi du côté de nos services fiscaux.

Même lorsque je suis connecté à mon compte d'impôt et que le système a accepté la preuve de qui je suis en ouvrant la session, il y a une analyse comportementale en arrière-plan pour voir comment je me comporte lorsque je suis sur ce site. Cela fait 15 ans que je me connecte régulièrement à mon compte d'impôt et que je l'utilise. Le système doit s'attendre à un certain comportement de ma part. S'il constate un changement, cela peut déclencher automatiquement un signalement indiquant que quelqu'un a peut-être piraté mon compte, et l'accès peut être refusé.

M. Ziad Aboultaif: L'Estonie est l'exemple le plus réussi à l'heure actuelle. Depuis combien de temps est-ce qu'on y utilise ce système? En avez-vous une idée?

● (0935)

M. Jerry Fishenden: On a commencé à le mettre en place au début des années 2000, je crois. Je ne sais pas exactement quand il est arrivé à maturité. Je crois qu'on continue de l'améliorer. Plus récemment, on a ajouté des cartes SIM sécurisées dans les téléphones mobiles, de sorte que le programme a évolué.

Vous feriez probablement mieux de vous adresser à eux pour obtenir des renseignements précis.

M. Ziad Aboultaif: Le risque que prend n'importe quel gouvernement qui essaierait de mettre en oeuvre ce genre de choses, c'est de révolutionner radicalement la façon dont se font les choses. Ensuite, si on essaie d'intégrer tout dans une même base, c'est le paradis pour les pirates, d'une certaine façon, puisqu'ils peuvent obtenir tous les renseignements dont ils ont besoin au même endroit. S'ils s'introduisent dans le système, les conséquences dépassent tout ce que vous aurez investi de coûts ou de mesures économiques.

À votre connaissance — j'ai lu votre exposé préliminaire et je l'ai écouté —, y a-t-il des exemples concrets indiquant que le système proposé est supérieur à ce que nous ou d'autres pays utilisons actuellement? Y a-t-il des preuves qu'il est préférable de prendre cette direction plutôt que de conserver le système actuel?

M. Jerry Fishenden: Je comprends bien le problème d'avoir tout au même endroit. On en revient presque toujours à Facebook et à Cambridge Analytica en ce moment, parce que c'est un excellent exemple de ce qui se passe quand quelqu'un a accès à toutes vos données au même endroit, et cela a des conséquences non seulement pour vous, mais aussi pour tout le cercle de vos connaissances.

Quant au modèle estonien, je pense qu'on pourrait adopter leur solution en y ajoutant ce dont parlait votre collègue, c'est-à-dire réfléchir aux moyens de laisser aux citoyens le contrôle du mode d'établissement de la preuve d'identité et de leur permettre ensuite de la relier aux autres services données pour qu'ils deviennent le point d'articulation de confiance. C'est en grande partie une question de confiance, et il s'agit d'obtenir que les citoyens aient confiance non seulement dans les intentions du gouvernement, mais aussi dans la technologie. Je crains que plus ils voient ce que font les entreprises du secteur privé avec la technologie, plus ils s'inquiètent des intentions du gouvernement à l'égard de ces données.

Il y a aussi le degré de propension au risque du gouvernement. Compte tenu de ce qui se passe du côté des documents imprimés, des risques qui y sont associés et des mesures d'atténuation qui ont été prises à leur égard, on peut se demander si nous n'attendons pas trop de la technologie ou si nous ne la surchargeons pas, parce que nous pensons qu'elle peut faire un meilleur travail.

J'ai toujours trouvé amusant, en signant ma déclaration d'impôt imprimée, qu'on ne m'ait jamais demandé un exemplaire de ma signature dès ma première déclaration, et je me demande bien ce que peut prouver ma signature dans ce cas. Cependant, lorsqu'on est passé au numérique, on s'est tout à coup préoccupé des signatures numériques ou électroniques. C'est peut-être nécessaire compte tenu du risque financier ou de l'exposition d'un ministère à certains risques, mais il peut y avoir de nombreux services pour lesquels le modèle de gestion des risques approprié consisterait à dire que nous comprenons les risques, que nous avons les mécanismes qui conviennent pour les gérer et que cela n'exige pas le niveau le plus élevé de preuve d'identité.

Le président: Merci.

Merci, Ziad.

La parole est maintenant à Mme Fortier. Vous avez cinq minutes.

[*Français*]

Mme Mona Fortier (Ottawa—Vanier, Lib.): Merci beaucoup.

Bonjour. Je vous remercie d'être ici aujourd'hui.

Vous avez déjà commencé à effleurer le sujet des cyberattaques. J'aimerais savoir si le modèle britannique prévient les cyberattaques actuellement? S'occupe-t-il de questions de sécurité précises dont vous pourriez nous faire part?

[*Traduction*]

M. Jerry Fishenden: Merci.

Je ne sais pas exactement ce que je peux vous dire sur les cyberattaques. Les ministères sont constamment attaqués par des robots et des agents automatisés. Nous avons également eu des attaques de déni de services distribués. Nous cherchons constamment des moyens de les contourner.

Nous avons la chance d'avoir le GCHQ et le Centre national de cybersécurité, qui savent très bien prévoir et prévenir les attaques et conseiller non seulement le gouvernement, mais aussi les entreprises du Royaume-Uni sur les mesures d'atténuation à prendre. Par ailleurs, en cas de cyberattaque ou de compromission de données, ils savent très bien quels conseils donner pour rétablir la situation afin qu'il n'y ait pas de dommages prolongés.

Il m'est difficile de donner des précisions. Je pense que vous aurez besoin d'une séance à huis clos avec un représentant du Centre national de cybersécurité au Royaume-Uni. Je fais simplement attention, surtout à titre personnel, à ce que je peux me permettre de vous communiquer.

● (0940)

[*Français*]

Mme Mona Fortier: Je le comprends et je respecte cela. C'était important de le souligner. Cela nous préoccupe dans le moment, car cela fait partie de nos analyses en vue de la transformation du système.

Par ailleurs, nous sommes devant le fait que les services gouvernementaux numériques sont un incontournable. Les Canadiens et les Canadiennes veulent de plus en plus de services numérisés — si on comprend bien la volonté de faire affaire avec les différents gouvernements. Comme nous l'avons mentionné plus tôt, il y a trois niveaux de gouvernement auxquels les citoyens peuvent s'adresser, soit le niveau fédéral, le niveau provincial et territorial et le niveau municipal. Nous devons tenir compte de cette complexité.

Vous avez déjà eu l'occasion de nous faire part de certaines idées, mais une des questions que je veux vous poser porte sur les conseils que vous pourriez offrir au gouvernement du Canada dans ses efforts en vue de numériser les services. Avez-vous d'autres conseils à nous donner ce matin?

[*Traduction*]

M. Jerry Fishenden: Merci.

Je pense que cela nous ramène à la première question de mon exposé préliminaire: qu'essayez-vous d'obtenir en passant au numérique? S'agit-il simplement de faire passer davantage de services en ligne et, en fait, de continuer à fonctionner avec des formulaires, où il ne s'agit plus d'imprimés, mais de formulaires informatiques, ou s'agit-il de trouver des moyens d'améliorer le modèle opérationnel du gouvernement proprement dit pour procéder à une vraie refonte des services?

Si nous avons de meilleures données au gouvernement, pourquoi demandons-nous aux citoyens de nous dire constamment des choses que le gouvernement sait déjà, par exemple où nous vivons, combien nous gagnons, combien d'enfants nous avons et si nous sommes mariés? Pourquoi ne pas privilégier davantage les services axés sur les données et les services utiles à la population au lieu de demander constamment aux gens de remplir des formulaires?

Je vois bien que l'intérêt semble s'orienter vers mon point de vue...

[*Français*]

Mme Mona Fortier: Au cours des 20 ou 30 prochaines années, la numérisation sera inévitable. On parle ici d'une transformation. Nous devrons être en mesure d'offrir plus rapidement et de façon sécuritaire des services aux Canadiennes et aux Canadiens. Il a été question de modèles qui existent déjà en Europe, notamment en Estonie, de même qu'en Australie.

Quel serait le conseil le plus important que vous auriez à nous donner, sachant que nous devrons vraiment nous engager dans cette transformation?

[*Traduction*]

M. Jerry Fishenden: Je pense que dans un monde idéal, je prendrais le temps de réfléchir et de me demander: « Comment voulons-nous que nos services publics fonctionnent et communiquent avec les citoyens dans les cinq à dix prochaines années? » Je prendrais le temps d'examiner toute la situation.

J'ai dit que les gens vont porter davantage d'appareils de surveillance médicale et que l'Internet des objets va se répandre dans les foyers et interagir constamment avec les gens. Il y a toute une série de changements à venir. Je crains que le gouvernement ne soit toujours en retard. Si, aujourd'hui, il envisage encore de transférer des choses sur des sites Web, alors que le reste du monde passe à l'Internet des objets et des appareils, le monde entier sera encore passé à autre chose au moment où le gouvernement rattrape le Web.

Je pense que c'est l'occasion de réfléchir. Nous avons un problème très semblable au Royaume-Uni entre le gouvernement central et le gouvernement local, et nous avons de multiples niveaux d'administration. C'est une occasion unique de simplifier considérablement les opérations internes au niveau local et au niveau central et d'investir davantage de ressources dans les services de première ligne.

Ce qui m'inquiète, c'est que nous parlons trop des services en ligne au lieu de penser en termes numériques la façon dont le gouvernement lui-même réorganise et restructure ses propres opérations pour en simplifier les processus, les fonctions et l'administration et ainsi simplifier les services de première ligne, qu'ils soient offerts en personne ou par un gadget quelconque. En faisant un meilleur usage de la technologie au gouvernement, on pourrait investir plus de ressources dans les services de première ligne qui ne peuvent peut-être pas être automatisés.

● (0945)

Le président: Merci, monsieur Fishenden.

Je demande l'indulgence du Comité. Il est maintenant 9 h 45, mais deux autres personnes ont des questions à poser, et nous avons là une excellente conversation. Nous avons dû réserver du temps, plus tôt, à une motion ou à une discussion. Accepteriez-vous de prolonger la séance de 10 minutes et de terminer les questions?

M. Nathaniel Erskine-Smith: Pour au moins une autre série.

Le président: Monsieur Fishenden, pouvez-vous rester encore 10 minutes?

M. Jerry Fishenden: Oui, bien sûr.

Le président: Nous allons passer à M. Picard.

Oui, monsieur Angus?

M. Charlie Angus: Eh bien, je suis ouvert à cette idée, mais je veux m'assurer que nous allons passer à la liste des témoins et à la neutralité d'Internet, parce que nous devons prendre aujourd'hui une décision concernant la liste des témoins.

Le président: Oui, c'est d'accord.

Allez-y, monsieur Picard, vous avez cinq minutes.

[*Français*]

M. Michel Picard (Montarville, Lib.): Je vous remercie.

Bonjour. Ma première question est très générale et concerne la transparence.

Il semble que tous ceux qui veulent des procédures ou une administration modernes parlent de l'importance de la transparence du gouvernement. Or c'est un cliché que personne ne définit ni ne précise. Si, pour des raisons de transparence, j'obtenais de l'information de nature financière du ministère des Finances, je pourrais influencer le marché de façon inappropriée. L'accès à de l'information de sécurité pourrait faciliter la commission d'actes terroristes.

Dans la recherche d'une meilleure transparence d'un gouvernement numérique, quelle est votre compréhension de ce que devrait être un gouvernement transparent?

[*Traduction*]

M. Jerry Fishenden: Merci.

Je pense qu'il y a peut-être plusieurs niveaux de réflexion. Il y a d'abord l'approche estonienne, dont nous avons parlé et selon laquelle les citoyens peuvent au moins voir qui a eu accès à leurs données ou qui les a utilisées. Ensuite, il y a la question plus vaste de savoir dans quelle mesure le gouvernement est prêt à divulguer beaucoup plus de données financières sur ses activités internes. Vous avez parlé de l'éventuelle menace que, s'il le faisait, des gens pourraient essayer de déjouer le système et de manipuler le marché. Par contre, cela nous permettrait peut-être de mieux comprendre où la fonction publique fait du très bon travail et où d'autres secteurs de la fonction publique pourraient suivre l'exemple d'une organisation donnée parce que son fonctionnement est très efficace sur le plan financier. Cela pourrait aussi nous permettre de voir où d'autres secteurs de la fonction publique ne fonctionnent pas aussi bien et de collaborer pour les améliorer.

De plus, à l'ère de l'informatique, il est possible de garantir un certain degré de transparence dans les algorithmes et les processus. Par exemple, concernant le calcul de l'aide sociale, le gouvernement garde-t-il ces processus pour lui ou permet-il à des tiers de gérer mes affaires financières en fonction d'un système de calcul de l'aide sociale? Les citoyens auraient beaucoup à gagner s'ils pouvaient communiquer leurs données financières à un conseiller financier. Si un conseiller financier pouvait modéliser ma situation en fonction des règles et des calculs du gouvernement, il pourrait m'aider à savoir si je peux demander des prestations ou si j'ai droit à un remboursement d'impôt ou quelque chose du genre.

Il y a de nombreux niveaux de transparence. Je pense que c'est une bonne question, parce que je ne pense pas avoir vu qui que ce soit y répondre. Dans quelle mesure le gouvernement veut-il s'engager dans l'ère numérique du point de vue du type d'information auquel il donne accès? Par ailleurs, dans quelle mesure donne-t-il certains de ses systèmes pour permettre à d'autres d'intervenir et d'aider le gouvernement à innover et à améliorer ses services?

● (0950)

[*Français*]

M. Michel Picard: Comparons nos systèmes à ceux de l'Estonie, par exemple. Nous vantons les mérites de systèmes extrêmement sophistiqués, qui tendent à garantir qu'ils sont sécuritaires à presque 100 % et que l'information donnée est exacte grâce à des contrôles et à de multiples contre-vérifications. Personnellement, je trouve que ce n'est pas un point à mettre en avant. C'est le minimum auquel on doit s'attendre dans l'état actuel de la technologie.

Les systèmes vont évoluer encore plus, mais il existe actuellement des systèmes extrêmement performants et dotés des meilleurs mécanismes de protection du monde contre une attaque de l'extérieur. Or aucune présentation sur des systèmes numériques efficaces, y compris celle des représentants de l'Estonie qui ont témoigné la semaine dernière, n'a parlé du seul risque incontrôlable: l'élément humain. Je n'ai pas de réponse non plus. Les systèmes sont de plus en plus complexes et le risque vient de plus en plus de l'intérieur, et non de l'extérieur. Pourtant, en dépit de l'élaboration de grandes procédures techniques, il n'est question d'aucune procédure pour faire face aux risques posés par les ressources humaines.

[*Traduction*]

M. Jerry Fishenden: Je conviens que le facteur humain reste un point faible dans beaucoup de ces systèmes. J'ai parlé plus tôt de l'ingénierie sociale dont nous avons été témoins lorsque des systèmes informatiques très sensibles ont été mal utilisés au Royaume-Uni. Bien que ces systèmes comprennent des mécanismes de surveillance qui déclenchent des alertes en cas d'accès inapproprié, le délai entre l'accès et le moment où l'on trouve le responsable est, hélas, parfois tragiquement long, et je l'entends littéralement: « tragiquement long », dans au moins un cas.

Le degré de propension au risque est une question récurrente, de même que tout ce qui touche au génie logiciel. Comment pouvons-nous faire confiance au code qu'un être humain a produit, tout au long du système jusqu'à l'exploitant? Comme cela peut être un point faible, comment s'assurer que le moins de données inutiles possible soient communiquées aux utilisateurs lorsqu'ils regarderont un écran au lieu de les laisser prendre connaissance de tout le dossier de quelqu'un sur un seul écran et tout voir en même temps?

Vous avez raison de dire qu'il faut tenir compte de tous ces éléments dans la conception de ces systèmes, mais, au bout du compte, il y aura toujours un risque. Dans quelle mesure êtes-vous prêts à prendre des risques, compte tenu des coûts et des mesures d'atténuation que vous êtes disposés à assumer dans chaque cas?

Le président: Merci, monsieur Picard.

Monsieur Angus, vous avez deux minutes pour terminer.

M. Charlie Angus: Ça va.

Le président: Merci à tous d'être venus, et surtout à M. Fishenden, qui nous vient du Royaume-Uni. Merci de votre témoignage. Nous serons heureux d'avoir d'autres discussions ultérieurement.

Nous allons suspendre la séance jusqu'au huis clos.

[*Les délibérations se poursuivent à huis clos*]