ASSEMBLÉE NATIONALE DU QUÉBEC

PREMIÈRE SESSION QUARANTE-DEUXIÈME LÉGISLATURE

Journal des débats

de la Commission permanente des finances publiques

Le mercredi 26 mai 2021 — Vol. 45 N° 133

Consultations particulières sur le projet de loi n° 95 — Loi modifiant la Loi sur la gouvernance et la gestion des ressources informationnelles des organismes publics et des entreprises du gouvernement et d'autres dispositions législatives (2)

Président de l'Assemblée nationale :
M. François Paradis

2021

Commission des finances publiques

Le mercredi 26 mai 2021 — Vol. 45 N° 133

Table des matières

Autres intervenants

M. Jean-François Simard, président

M. Éric Caire
M. Gaétan Barrette
M. Vincent Marissal

* Mme Nicole Martel, AQT
* M. Alain Lavoie, idem

* Témoins interrogés par les membres de la commission

Le mercredi 26 mai 2021 — Vol. 45 N° 133

Consultations particulières sur le projet de loi n° 95 — Loi modifiant la Loi sur la gouvernance et la gestion des ressources informationnelles des organismes publics et des entreprises du gouvernement et d'autres dispositions législatives (2)

(Onze heures trente-quatre minutes)

Le Président (M. Simard) : Alors, chers amis, bienvenue en direct de la salle La Fontaine de l'Assemblée nationale du Québec. Je constate que nous avons quorum. Les travaux de la Commission des finances publiques peuvent donc débuter.

Comme vous le savez, nous sommes réunis de manière virtuelle afin de procéder aux consultations particulières et aux auditions publiques sur le projet de loi n° 95, Loi modifiant la Loi sur la gouvernance et la gestion des ressources informationnelles des organismes publics et des entreprises du gouvernement et d'autres dispositions législatives.

Mme la secrétaire, bonjour. Y aurait-il des remplacements ce matin?

La Secrétaire : Non, M. le Président, aucun remplacement.

Auditions (suite)

Le Président (M. Simard) : Aucun remplacement. Voyez-vous, même si on est un à côté de l'autre, ça se fait de manière virtuelle, alors il y a toujours un léger décalage.

J'aurais besoin, avant d'aller un peu plus loin, de deux consentements, le premier, pour fonctionner un peu comme hier, finalement, et de répartir le temps que ne prendra pas le Parti québécois équitablement entre le Parti libéral et le représentant de Québec solidaire. Y a-t-il consentement? Consentement.

Et j'aurais besoin d'un autre consentement afin de poursuivre au-delà de l'heure prévue nos travaux puisque, malheureusement, nous commençons légèrement en retard.

Une voix : Consentement.

Le Président (M. Simard) : Très bien. Alors, nous sommes... Nous commençons notre journée en recevant les représentants de l'Association québécoise des technologies. Alors, madame, monsieur, soyez les bienvenus. Merci de vous joindre à nous. Auriez-vous d'abord l'amabilité de vous présenter?

Association québécoise des technologies (AQT)

Mme Martel (Nicole) : Bonjour. Mon nom est Nicole Martel. Je suis présidente-directrice générale de l'Association québécoise des technologies, aussi connue sous l'AQT, et je suis accompagnée de M. Alain Lavoie, qui est président de la compagnie Irosoft. C'est une entreprise de technologies de l'information. Et M. Lavoie est également membre du conseil d'administration de l'AQT.

Le Président (M. Simard) : Merci. Alors, vous disposez de 10 minutes.

Mme Martel (Nicole) : Alors, bien, merci. Merci, M. le Président. Merci de nous accueillir, chers députés membres de la commission. Donc, on espère que nos commentaires, aujourd'hui, contribueront à vos réflexions et qu'ils pourront aider le gouvernement à mener à bien cet important projet de loi.

Bien, je vous dirais déjà sans détour que, dans le cadre de mon travail, je découvre encore, à tous les jours, des technologies qui, de façon très innovante, aident le quotidien des entreprises et des individus.

Je suis également à même de constater l'évolution à vitesse grand V du secteur, des besoins, de la demande, mais aussi des enjeux qui mettent en perspective toute l'importance de la numérisation des données et surtout de la saine gouvernance de celles-ci.

C'est donc avec optimisme que nous entrevoyons la transformation numérique des organismes publics. Et on comprend que, pour optimiser les services aux citoyens et entreprises, les ministères et organismes devront se doter d'un cadre de gestion qui implique le partage des données.

D'abord, un mot pour préciser le rôle de l'AQT et notre composition, dans le fond, du secteur québécois des technologies. L'écosystème des technos touche tous les domaines et expertises, par exemple, les télécommunications, les services informatiques, les logiciels en passant par les notions d'intelligence artificielle et tous les autres aspects de la transformation numérique. L'importance du secteur techno, au Québec, est indéniable. On dénombre 154 000 emplois professionnels répartis dans environ 2 000 entreprises. Plus des deux tiers des membres de l'AQT s'illustrent par des ventes hors Québec, signe que l'expertise de nos solutions, de nos produits sont reconnus sur la scène mondiale.

Un fait peut-être méconnu par plusieurs, nos entreprises technos transigent avec des instances privées ou publiques, dont les exigences de sécurité sont très élevées, que ce soit ici ou ailleurs. Plusieurs entreprises locales,

québécoises ont déjà des accréditations de sécurité et de conformité telles que le RGPD et autres conformités très élevées, et ce, depuis plusieurs années.

Donc, je l'ai mentionné un peu plus tôt, l'évolution du secteur techno et la numérisation des données évoluent rapidement. Les entreprises, tout comme les gouvernements, ont donc le devoir d'adapter leurs façons de faire non seulement pour garantir une meilleure efficacité et une meilleure efficience pour les Québécois, mais également pour assurer la sécurité et une confidentialité, qui est attendue des citoyens, auxquelles ils ont droit.

Ce mouvement de transformation numérique, eh bien, il est inévitable et il est déjà bien entamé. Il est en voie aussi d'être bien ancré dans les habitudes de vie des Québécois, Québécois qui demandent aujourd'hui un service de qualité et exigent une rigueur quant aux informations détenues par le gouvernement.

Il faut reconnaître que la circulation des données n'est pas sans risque. Les dernières années, il y a eu des nombreux vols de données qui ont défrayé les manchettes. Autant les entreprises privées que les institutions publiques ont été touchées, et malheureusement personne n'est à l'abri de tels risques. C'est pourquoi on salue le projet de loi n° 95, qui vient encadrer les modes de fonctionnement du futur en matière de circulation et gestion de l'information.

Donc, pour bénéficier des avantages, les citoyens doivent avoir une confiance indéniable face à l'État et à l'utilisation de leurs données.

• *(11 h 40)* •

Donc, il y a quelques éléments sur lesquels nous désirons attirer votre attention. D'abord, à l'article 12.2, alinéa deux, il est prévu qu'un organisme public se doit d'apporter les corrections quant à une situation, et sans tarder, advenant une atteinte d'intégrité à des renseignements personnels. Donc, ça va de soi. Nous irions plus loin et nous considérons qu'il y a nécessité d'informer les citoyens, entreprises si leurs données sensibles ont été compromises, d'ailleurs, comme il est prévu dans le projet de loi n° 64.

Quant à la création des nouveaux rôles, nous sommes d'accord avec la création des trois nouveaux rôles qui sont confiés au DPI, au dirigeant principal de l'information, donc soit le chef gouvernemental de la sécurité de l'information, le chef de la transformation numérique ainsi que le gestionnaire des données numériques, comprenant qu'il est important qu'il y ait une personne qui ait une vue d'ensemble sur tous les projets confiés aux différents ministères et organismes. Donc, ces nouveaux rôles qui seront confiés au DPI occasionnent de très importantes responsabilités additionnelles, puis on estime qu'il est nécessaire que les ressources et des budgets supplémentaires soient accordés et mis... pour la mise en application de ce nouveau cadre de gestion. Selon nous, il est essentiel de prévoir... appelons-le création d'un centre d'expertise. Pour que des ressources y soient dédiées, nous sommes d'avis que notre État doit avoir des ressources affectées à 100 % de leur temps à ces questions, donc la cybersécurité, la gouvernance des données, la transformation numérique, en d'autres mots, bien, se donner les moyens de nos ambitions.

Nous estimons aussi que ce p.l. ne doit pas être perçu uniquement comme un projet techno, mais plutôt comme un projet de gestion de changement où il sera important de former et de rehausser les expertises des individus qui traiteront les données. Il sera important de bien communiquer au sein même des organismes pour que ce nouveau cadre de gestion soit compris de tous et que, peu importe leur rôle, que ce soit les avocats, les informaticiens, les agents d'information, les préposés au service à la clientèle, soient bien informés de ce nouveau cadre de gestion. Il sera important de bien communiquer la classification déjà en vigueur au gouvernement du Québec quant aux autorisations et aux types de données et fournir les habiletés nécessaires pour les traiter.

Ce qui m'amène à parler des collaborations qui sont nécessaires entre l'État et les entreprises technologiques issues du privé, qui représentent un véritable écosystème, qui est certainement un des éléments qui pourra contribuer aussi au succès par la suite. Donc, l'AQT croit fermement que nous devons miser sur ces collaborations et continuer de les faire grandir. Pour nous, il est clair que le rehaussement nécessaire de la sécurité des données n'est pas lié à la nature de l'organisation qui détient ces données, mais plutôt au processus qui est mis en place et au respect rigoureux de celui-ci. Si le développement d'une expertise de pointe au sein même du gouvernement est primordial pour relever les défis actuels et ceux à venir, il peut sans conteste être accompagné de partenaires qui détiennent aussi ces expertises et qui les développent au quotidien.

L'optimisation de la gouvernance pour réaliser l'ambition du gouvernement en la matière passera aussi par le renforcement de l'expertise des partenaires et des fournisseurs. C'est dans ce sens que nous croyons que le ministère de l'Économie pourrait créer un programme pour permettre aux entreprises de se conformer au nouveau cadre. Il faut qu'on favorise cette collaboration, notamment en créant des espaces d'échange pour identifier des bonnes pratiques, les bonnes certifications, et moduler certaines mesures de validation des expertises pertinentes, par exemple, en créant un comité aviseur composé de gens du privé et du public.

En terminant, nous croyons que miser sur le savoir-faire québécois, sur nos experts, sur nos PME, sur nos entreprises, c'est miser sur l'enrichissement collectif et le rehaussement de nos expertises.

Alors, merci de votre écoute. Nous sommes prêts à échanger et répondre à vos questions avec M. Lavoie. Merci.

Le Président (M. Simard) : Merci à vous, Mme Martel. Et, compte tenu du temps pris pour votre présentation, le gouvernement dispose de 17 minutes. M. le ministre.

M. Caire : Merci, M. le Président. M. Lavoie, Mme Martel, merci d'être là, merci de cette présentation. M. Lavoie, vous me permettrez quand même de m'étonner de votre mutisme. Je ne vous ai jamais connu aussi discipliné, parce qu'on a eu l'occasion de vous entendre en commission parlementaire sur le projet de loi n° 14 et sur le projet de loi n° 37, donc je salue votre gentilhommerie. On va le voir comme ça.

Donc, j'ai plusieurs éléments que je voulais aborder avec vous. Dans un premier temps, peut-être répondre à certaines interrogations qui étaient dans le mémoire, puis, après ça, je vais vouloir échanger avec vous, notamment sur les partenariats entre le public et le privé qui soulèvent, pour moi, des grandes interrogations compte tenu de la nature du projet de loi n° 95.

Puis je vais peut-être commencer par ce commentaire que vous avez sur la divulgation des incidents de confidentialité. Vous faites référence au projet de loi n° 64, et je vous en remercie parce que ça me permet de réitérer que cette notion-là n'a pas à être incluse au projet de loi n° 95 justement parce qu'elle est incluse au projet de loi n° 64 et que le projet de loi n° 95 est entièrement soumis aux dispositions de n° 64. Et on l'a mise, cette disposition-là, on la met dans 64 parce que le projet de loi n° 64 s'adresse à l'ensemble des organismes publics, alors que la Loi sur la gouvernance et la gestion des ressources informationnelles s'applique aux organismes du gouvernement et aux entreprises du gouvernement seulement. Donc, 64, c'est tous les organismes publics, incluant municipaux, ordres professionnels, etc., plus les entreprises privées. Donc, c'est les deux lois. Donc, cette disposition-là, elle est donc couverte beaucoup plus largement par le projet de loi n° 64.

Autre élément que vous apportez, c'est la question de... Bien, en fait, vous parlez du chef de la sécurité et vous parlez des différentes entités qui sont créées et des budgets qui seraient nécessaires. En fait, le projet de loi n° 95 officialise des fonctions qui existent déjà autrement mais administrativement au sein du gouvernement et des fonctions qui, du point de vue administratif, ont une autorité, et une légitimité, et un rayon d'action beaucoup plus limités.

Donc, on vient légiférer pour justement s'assurer que ces officiers-là, qui vont être incarnés par le DPI... Mais on peut comprendre qu'il y a un pouvoir de délégation qui vient avec. C'est un pouvoir, donc, qui est prévu par la loi, et donc ce pouvoir-là s'étend maintenant à l'ensemble des organismes touchés par la LGGRI. Donc, il n'y a pas besoin de budgets supplémentaires qui n'ont déjà été octroyés avec l'adoption de la politique de cybersécurité parce qu'on ne crée pas de nouveaux postes, au sens propre. Donc, là-dessus, je voulais vous rassurer, là, les budgets ont déjà été accordés, puis c'est vraiment... on voulait s'assurer qu'il y ait une autorité pour ces officiers-là mais en vertu de la loi. Donc, ça, c'était un élément que je voulais préciser.

Vous amenez un élément intéressant, et, vous le savez, on a eu des discussions dans le passé, moi, je ne suis pas hostile aux collaborations avec l'écosystème, milieu académique, milieu de recherche, entreprises privées et gouvernement. Mais là vous venez me chercher, au sens où, et je veux vous entendre là-dessus, pour moi, il y a des fonctions, excusez l'expression, mais régaliennes d'une organisation qui ne peuvent être partagées. Et la sécurité des systèmes d'information d'une organisation, qu'elle soit privée ou publique, ma vision de ça, c'est quelque chose qui doit être assumé entièrement par l'organisation. Et donc la sécurité des systèmes d'information du gouvernement, la sécurité des données qui sont confiées au gouvernement par les citoyens et la sécurité des actifs critiques du gouvernement, à titre d'organisation, devraient relever exclusivement du gouvernement et de ses officiers à l'interne.

Vous semblez, vous, dire qu'il y a là des opportunités de collaboration. J'aimerais ça vous entendre là-dessus puis j'aimerais ça que vous me précisiez ce que vous entendez par là. Parce qu'à l'inverse une grande entreprise ferait-elle ça, partager ses secrets, partager ses responsabilités de sécurité avec une autre entité? J'aimerais ça vous entendre là-dessus.

Le Président (M. Simard) : Mme Martel.

M. Lavoie (Alain) : Je vais prendre...

Mme Martel (Nicole) : Je demanderais...

Le Président (M. Simard) : Ah! M. Lavoie, alors.

Mme Martel (Nicole) : Je vais demander à M. Lavoie d'intervenir.

Le Président (M. Simard) : M. Lavoie.

M. Caire : Je me disais qu'il était beaucoup trop discret.

M. Lavoie (Alain) : Écoutez, pour vous répondre...

Le Président (M. Simard) : M. Lavoie, excusez-moi. Simplement pour les fins de notre procès-verbal, auriez-vous l'amabilité de vous représenter, s'il vous plaît?

• *(11 h 50)* •

M. Lavoie (Alain) : Mon nom est Alain Lavoie. Je suis président de la compagnie Irosoft et je suis membre du conseil d'administration de l'AQT.

Donc, pour répondre à votre question, essentiellement, la réalité, M. le ministre, c'est qu'on est dans un contexte de pénurie de main-d'oeuvre, au Québec, en technologies de l'information. Et nous, à l'AQT, on voit ça un peu comme dire : On est condamnés à travailler les deux ensemble, le gouvernement et l'industrie, dans le futur, et... parce qu'il va manquer de main-d'oeuvre un peu partout. Et le gouvernement va devoir... Il va y avoir des opportunités pour que le gouvernement travaille aussi avec les entreprises pour le futur. Donc, il faut... Quand on dit «des collaborations», on ne parle pas ici, essentiellement, de donner ses données ou donner des responsabilités, mais il va falloir travailler avec des fournisseurs dans le cadre de... dans le futur. Et c'est dans ce contexte-là qu'on voit les collaborations, à ce stade-ci, avec le p.l. n° 95.

Ceci dit, on voyait très bien que le p.l. n° 95... En fait, la beauté du p.l. n° 95, pour nous, c'est un peu... c'est une réponse au p.l. n° 64 en disant : Regardez, on a mis le p.l. n° 64, maintenant on va établir les rôles et responsabilités des parties prenantes des ministères et organismes, des règles du jeu quant à la gestion et la circulation des données entre les ministères, mais ce modèle-là du p.l. n° 95, bien, il risque, du même coup, d'être adapté au processus dans le contexte industriel aussi parce que... Écoutez, pour les PME, et surtout pour les PME et les start-up, principalement, mais aussi pour toutes les industries, quand ils vont dire : Bien, écoutez, comment on comprend, on n'a peut-être pas tous les moyens de se conformer au p.l. n° 64, on ne se peut pas payer des experts pour nous aider à faire ça, bien, on va faire le même modèle que le gouvernement dans ce contexte-là.

Donc, ça, il faut que vous ayez à l'esprit ça, que le p.l. n° 95 est le modus operandi que vous allez mettre en place au gouvernement, va être probablement mimé par les industries, surtout pour les PME et les start-up, qui vont être... vous allez être un modèle pour eux. Et essentiellement il faut que ça soit simple, il faut...

Puis quand on demande... quand on parle de budget, M. le ministre, c'est qu'il va falloir faire comprendre à toute personne qui va manipuler de la donnée, et non pas seulement des informaticiens et des experts, mais il va avoir besoin d'une très bonne communication pour comprendre pourquoi qu'on fait ça puis comment on le fait correctement pour que ça facilite le modus operandi, qu'on comprenne pourquoi on ne touche pas à cette donnée-là, on ne la rend pas disponible ou pourquoi on la met disponible, ces choses-là. Et ça, il faut que ça soit clair, pour que ça perdure, pour que ça... je dirais un mot que j'ai utilisé souvent dans d'autres commissions, pour que ça percole dans la machine, bien, il faut essentiellement que ça soit bien expliqué à tout le monde du gouvernement. Et ça, ça va devenir un modèle pour l'industrie. C'est dans ce contexte-là qu'on voit les collaborations entre les deux.

M. Caire : Mais je vais quand même, M. Lavoie, Mme Martel, je vais quand même faire un peu de millage sur ce que vous avez dit au début de votre intervention. Oui, je pense que ce modèle de gouvernance là peut faire école, je n'en ai aucun doute.

Mais, ceci étant, je reviens sur la question du partage des ressources. Je l'entends, on la voit, on la ressent, la pénurie, mais, en même temps, où est-ce qu'on trace la ligne entre une organisation qui met sa sécurité à risque par une collaboration et des organismes qui partagent, pour leur plus grand bénéfice mutuel, les ressources? Je ne sais pas si vous comprenez ma question. Parce qu'il arrive un temps où se replier sur soi-même, je l'entends, ce n'est peut-être pas le modèle idéal, mais le bar ouvert ne m'apparaît pas non plus être la panacée. Ça fait qu'où est-ce qu'on la trace, cette ligne-là? Où est-ce qu'on partage l'expertise et où est-ce qu'on commence à se mettre à risque par rapport à cette ouverture-là?

Mme Martel (Nicole) : Je peux peut-être ajouter un complément d'information. Si la compréhension que vous avez eue de notre commentaire était à l'effet qu'on souhaitait partager des données avec le privé, ce n'était pas ça, le sens du commentaire. C'était plutôt de dire : On le sait, là, la pénurie de talents, ça nous touche tous de front. Qu'il y ait certaines expertises, que ce soit en cybersécurité, que ce soit en gouvernance des données, je pense que le gouvernement ne pourra pas, jamais, prétendre avoir l'ensemble de ces expertises-là dans son sein même, à l'interne. Donc, vous allez inévitablement vous tourner vers l'externe parce qu'il y a des entreprises dont c'est la vocation, par exemple, de faire ce type... de développer ce type d'expertise là. Alors là, peut-être qu'il faudrait prévoir des mécanismes par lesquels...

Vous avez déjà des catégories de niveaux de sécurité, là, qui fait en sorte que certains profils, dans vos ministères et organismes, sont habilités ou sont autorisés à traiter. Puis certains types de données, plus les niveaux sont élevés, plus la sensibilité de la donnée est autorisée, bien, il faudra peut-être prévoir ce même mécanisme là pour les entreprises, les collaborateurs du secteur privé qui travailleront avec vous, là.

M. Lavoie (Alain) : Et si je peux...

M. Caire : ...

M. Lavoie (Alain) : Si je peux me permettre... Excusez-moi.

M. Caire : Oui, oui. Allez-y, M. Lavoie. Allez-y.

M. Lavoie (Alain) : Si je peux me permettre, c'est que les entreprises privées font ça depuis... depuis tout le temps, là, qu'ils travaillent avec le gouvernement.

M. Caire : Quand vous dites qu'ils font ça, M. Lavoie, pour que je comprenne bien, ils font quoi, «ça»?

M. Lavoie (Alain) : Qu'ils travaillent dans des mandats, qu'ils travaillent dans des mandats avec le gouvernement à titre de consultants ou à titre de fournisseurs, où il y a de la donnée sensible à l'intérieur de ces contrats-là, où on a tous... Moi, j'ai toujours dit : J'ai une épée Damoclès au-dessus de la tête. J'ai des contrats, là, qui fait que, s'il y a une brèche de sécurité ou une fuite de sécurité, bien, ça peut mettre à risque ma compagnie. Ça, ça a toujours été... puis le gouvernement a toujours mis des dispositions par rapport à ça. Vous avez classé vos données d'une certaine façon qui vous permet de...

Donc, on est habitués de faire ça. Ce n'est pas... On n'est pas en train de réinventer des choses, là, ça existe déjà. L'idée, c'est il faut que ce soit bien circonscrit dans la modernisation de ce que vous faites avec le p.l. n° 95 pour que

l'industrie continue à travailler de cette façon-là, comme on travaillait avant. Moi, je... À moins que je découvre de quoi, là, mais il me semble que ça faisait partie du paysage...

M. Caire : Absolument, mais, dans le contexte de 95, mon questionnement était parce que... ce que le gouvernement du Québec fait avec 95, puis je pense que vous l'avez bien établi, il établit une nouvelle gouvernance sur la sécurité de l'information. Donc, les collaborations qu'on a, par exemple, dans la conception, le déploiement de SAGIR, ce n'est pas de ça dont je vous parle, là. Et il y a différents contrats qui sont donnés à des entreprises de consultants au gouvernement du Québec, mais ce n'est pas de ça dont je parle, justement, parce que 95 ne parle pas de ça. 95 ne s'adresse pas à ces situations-là. 95 s'adresse à une situation interne où deux organismes publics ne s'échangent pas d'information, ce faisant, oblige chaque organisme à collecter cette information-là, surmultipliant des bases de données complètes, surmultipliant les risques de fuite, etc.

Donc, le modèle de gouvernance qu'on met en place, il s'adresse vraiment à la mécanique interne du gouvernement du Québec dans la circulation de sa donnée, dans la protection de sa donnée, dans la sécurité de ses systèmes d'information et dans sa transformation numérique. Donc, c'est pour ça que moi, j'excluais du périmètre de notre discussion les collaborations que nous avons déjà avec l'entreprise parce que ces collaborations-là ne sont pas impactées par 95.

Par contre, quand vous me parlez de collaboration dans le cadre de 95, c'est là où je suis moins sûr que je comprends. Quand on parle de déployer un réseau de sécurité interne, comment je peux collaborer avec l'entreprise privée? Est-ce que je laisse, par exemple, l'entreprise privée gérer un de mes centres de données? Est-ce que c'est ça dont vous nous parlez? Est-ce que je laisse une entreprise privée établir les accréditations de mes employés? Est-ce que c'est de ça dont vous parlez? C'est là où je suis moins à l'aise de parler de collaboration.

Mais peut-être que ce n'est pas de ça dont vous parlez. Ça fait que c'est pour ça que je voulais vraiment circonscrire le débat par rapport à ce qu'on fait dans 95.

M. Lavoie (Alain) : On n'allait pas jusque-là, M. le ministre, dans le cadre de nos représentations, mais il faut comprendre que p.l. n° 14, p.l. n° 64, p.l. n° 95 et les autres p.l. qui vont arriver, vous êtes en train de... bon, pour prendre l'expression consacrée, vous êtes en train de construire un avion en volant. Et là, bien, pour avoir toute l'idée... puis là on se dit : Bien, éventuellement, il va y avoir ces collaborations-là qu'on parlait, qui ne sont pas dans le périmètre de 95, mais qui vont être impactées par ce que vous mettez, par contre...

• *(12 heures)* •

M. Caire : Je comprends. Donc, dans le fond, ce que vous nous dites, là, c'est que vous souhaitez justement que 95, à l'intérieur de sa mission, ne vienne pas diminuer ou ne vienne pas empêcher les collaborations dans les autres sphères des missions de l'État où, là, une expertise pourrait ne pas être détenue par l'État et pourrait être sous-contractée à une entreprise privée. Dans le fond, ce n'est pas tant d'avoir de nouvelles collaborations que de ne pas mettre à risque les anciennes collaborations que nous avions déjà.

M. Lavoie (Alain) : Vous comprenez que vous avez des principes, comme les données officielles, la responsabilité des ministères et organismes qui pourraient faire qu'à un moment donné on dise : Bien non, on ne fera pas affaire avec le privé à cause qu'on a mis un processus en place. Et c'est pour ça que je reviens sur ce que j'ai dit au début, c'est : Il faut faire attention parce que ça peut être un modèle aussi. Il faut faire attention. Si le gouvernement commence à mettre des barrières pour travailler avec les entreprises, avec des PME, et les start-ups, et l'industrie, bien, ça peut faire la même chose avec les grands donneurs d'ouvrage, dans le privé, qui peuvent avoir peur que le p.l. 64 vienne leur taper sur les doigts, puis ils disent : Bien, on va faire la même chose que le gouvernement puis on ne donnera pas, essentiellement, les autorisations pour travailler avec ces données-là. C'est uniquement...

M. Caire : Quand vous dites, M. Lavoie... parce que je vois le temps qui file, je voulais vous poser une dernière question. Quand vous dites que p.l. 95 pourrait inspirer une nouvelle gouvernance dans l'entreprise privée, qu'est-ce qui vous inspire, là-dedans, particulièrement? Qu'est-ce que vous voyez d'exportable pour l'entreprise privée?

Le Président (M. Simard) : Alors, succinctement, très succinctement, s'il vous plaît.

M. Lavoie (Alain) : En fait, on pourrait s'inspirer des rôles qui ont été nommés là-dedans et de la reddition de comptes qui a été nommée là-dedans, qui fait que, si on fait une même reddition de comptes des... peut-être un peu plus petit pour des PME, mais, essentiellement, qu'on ait les mêmes rôles, essentiellement, dans une entreprise, bien, on est en mesure de se conformer à 64...

Le Président (M. Simard) : Merci. Alors, je cède maintenant la parole au député de La Pinière, qui dispose de 12 m 45 s. Cher collègue, il faudrait ouvrir votre micro.

M. Barrette : Merci, M. le Président. Alors...

Le Président (M. Simard) : Vous qui avez une si belle voix, aussi bien en profiter.

M. Barrette : Vous avez bien raison, M. le Président. Tu sais, je trouve qu'on vient d'assister à un échange intéressant. Je comprends pas mal votre position, mais, pour être bien sûr, encore plus, de la comprendre, vous souhaitez sous-traiter les activités prévues à 95?

Le Président (M. Simard) : M. Lavoie... ou Mme Martel, enfin.

M. Lavoie (Alain) : Nicole, vas-y.

Mme Martel (Nicole) : Ce n'est pas ce qui est prévu. Ce n'est pas de sous-traiter les activités qui sont prévues au p.l. n° 95, mais ce qu'on veut s'assurer... c'est que, s'il y a des mécanismes qui sont mis en place à l'interne pour traiter ou classifier certaines autorisations en fonction de la sensibilité des données, on voudrait que cette classification-là puisse être adaptée aussi, dans l'éventualité où vous travaillez avec des ressources externes à l'organisation qui sont requises dans la conduite de certains mandats, puis de ne pas nécessairement exclure le fait qu'on puisse faire appel à des expertises externes, mais plutôt prévoir un mécanisme par lequel des ressources externes auraient des autorités semblables à celles qui sont prévues pour les gens de l'interne.

M. Barrette : Oui, mais vous ne trouvez pas que ça revient un petit peu au même?

Mme Martel (Nicole) : On ne demande pas à ce que vous... que le gouvernement impartisse, tu sais, la réalisation des tâches d'échange de données. Ce n'est pas de l'impartition de fonction, c'est plutôt de s'assurer que, s'il y a des compléments externes qui sont requis à l'interne, qu'on prévoie des mécanismes par lesquels les ressources pourront avoir des accréditations semblables, toujours pour respecter les plus hauts standards de sécurité, là. Ce n'est pas de diminuer les standards ou quoi que ce soit, là.

M. Barrette : Ah! moi, je n'ai pas compris ça comme ça, je ne l'insinue pas du tout, là. Je pense qu'au Québec il y a l'expertise nécessaire pour rencontrer les plus grands standards, en termes de sécurité. Puis mon impression, compte tenu des travaux qu'on a faits précédemment dans deux autres projets de loi, est à l'effet que le ministre pense la même chose. Mais j'écoutais l'échange puis j'avais comme l'impression que vous vouliez avoir un rôle plus direct dans l'application du projet de loi n° 95.

M. Lavoie (Alain) : Non.

Mme Martel (Nicole) : Désolée, si c'est l'impression qu'on vous a laissée.

M. Barrette : Ah! mais c'est peut-être moi qui ai mal compris. Faites-vous-en pas, ça arrive, là.
Est-ce que vous avez eu la chance ou la malchance, c'est selon le temps que ça vous aura pris, de suivre nos travaux depuis hier?

M. Lavoie (Alain) : Un peu.

M. Barrette : Un peu. Est-ce que, sur le plan de l'architecture de la sécurité du traitement de données qui aurait été évoqué par plusieurs personnes, là, M. Waterhouse, M. Cuppens, M. Gambs, là, tous les gens qui ont parlé de ça hier, est-ce que vous êtes confortable avec ça? Avez-vous des commentaires additionnels à faire?

Mme Martel (Nicole) : J'inviterais M. Lavoie à répondre.

M. Lavoie (Alain) : En fait, écoutez, c'est des grands experts, là, qui ont passé hier. Essentiellement, je ne voudrais pas avoir la prétention d'avoir la même expertise. Il y a quand même un enjeu qui a été nommé, sur le croisement des données, là, essentiellement, là, hier, là, que vous avez discuté. Quand je regardais ça, je me disais, on parle... c'est un film que j'ai déjà vu, essentiellement. Rappelez-vous, au tournant de 2010, quand on a parlé de l'«open data», où on devait essentiellement ouvrir nos données à tout le monde pour la transparence de nos gouvernements, c'est Barack Obama qui a lancé ça, essentiellement, et tous les gouvernements. Et une des choses qu'on militait à ce moment-là, c'est dire : Écoutez, la main gauche puis la main droite d'un gouvernement peuvent avoir des données, O.K., qui sont mutuellement exclusives, mais... qu'on peut décider de les publier d'un côté puis de les publier de l'autre côté, mais, en les mettant ensemble, pourraient avoir des effets importants, et pour ça... Puis il y a même des grands chercheurs, là, qui ont... je faisais des conférences, au tournant de 2012, 2013, là-dessus, il y a même des chercheurs qui ont dit, bien, qu'il est possible de prendre de la donnée anonymisée qui vient des réseaux sociaux et de la ramener avec un pourcentage d'erreur très minime.
Ce que j'essaie d'amener là-dedans, c'est que, dans un contexte de... quand les gens ont parlé du croisement puis de la difficulté, j'ai vu... Moi, j'ai siégé sur des comités où il y avait des comités conjoints avec le public et avec des gouvernements, qui faisaient qu'on regardait à ce qu'une donnée qu'on rend publique, on peut la mettre en commun, et qu'on ait des experts, qu'il y ait un comité interministériel, des spécialistes de la donnée qui sont capables de dire : Attention! Celle-là avec celle-là pourrait faire des... puis qu'on est capables de discuter de ces données-là et des enjeux par rapport à ça.
Je pense que le p.l. n° 95 se préoccupe de ça aussi puis qu'il va pouvoir avoir ça. Avec les fonctions qu'on a mises, je pense que des gens vont pouvoir y réfléchir, mais c'est ça, il va y avoir des comités interministériels, et aussi avec l'industrie, qui ont aussi leurs façons de faire, qui vont pouvoir aider dans ce sens-là. Ça, je pense que c'était une chose, donc, un comité aviseur aussi qui pourrait être mis en place, qui pourrait être intéressant pour cette gouvernance des données là. Ça, je pense que c'est essentiellement...

Pour ce qui est de... Il y avait eu aussi des commentaires sur la question de la catégorisation des données, DIC versus les grilles d'impact au Québec, versus celles qui sont au fédéral. Je vous dirais, encore une fois, puis je reviens sur ce qu'on a dit au début, formation des gens, il faut savoir pourquoi et comment. Et changer, de façon drastique, des choses peut être compliqué, dans la gestion du changement, pour le mettre en application. Ça, c'est une des choses qu'on rencontre souvent dans l'implantation de grandes mesures comme ça. Il faut que les gens, les fonctionnaires, les avocats, tout le monde comprenne très bien pourquoi ils le mettent en place, pourquoi la donnée, il faut la protéger, pourquoi et comment la protéger.

Et donc, à savoir... parce qu'il semblait y avoir des discussions, à savoir, DIC versus celles du fédéral. Moi, je connais les deux, j'ai la... au fédéral. Peut-être qu'il pourrait y avoir des collaborations, entre autres, pour les qualifications, par exemple, entre des gens qui travaillent, mais sinon, je dis juste faire attention pour que ça soit facile à implanter. Le nerf de la guerre dans ce projet-là, c'est l'implantation, et non pas la techno. Puis je pense que, M. Barrette, vous êtes conscient de ça, que ce n'est pas facile, d'entrer une nouvelle politique à l'intérieur d'une machine aussi importante que le gouvernement.

M. Barrette : Ça, vous avez raison. Vous dites : Le nerf de la guerre, c'est... et non pas... Le deuxième mot que vous avez dit, j'ai mal entendu.

M. Lavoie (Alain) : Le nerf de la guerre, c'est l'implantation de ce cadre-là, correctement, que ça percole et que ce soit accepté.

• *(12 h 10)* •

M. Barrette : Non, ça, ça va, mais vous avez dit : et non pas...

M. Lavoie (Alain) : Je ne me rappelle pas. Je ne me souviens...

M. Barrette : ...je n'ai pas saisi.

Mme Martel (Nicole) : C'est parce que ce n'est pas un problème technologique, ce n'est pas un danger technologique, mais c'est plutôt un enjeu humain, de gestion de changement.

M. Lavoie (Alain) : Humain.

M. Barrette : Oui. Ça, disons qu'hier j'ai fait la remarque, là, je pense que vous allez être d'accord avec ça, 95, ça a une grande envergure, et, en quelque part, il faut qu'absolument tout le monde dans tous les ministères et organismes marche au même pas pour qu'on arrive au résultat escompté de façon sécuritaire, sinon on aura ce que j'ai appelé des talons d'Achille, à gauche et à droite, là, et ça risque de s'écraser, ça, tout ça. En tout cas, il risque d'y avoir des événements de sécurité, comme on a dit.

Vous, ce que vous nous... quand vous nous regardez, là, quand... bien, nous étant l'État, là, pas moi, personnellement, là, bien, essentiellement, ce que vous nous dites aussi, c'est un peu une mise en garde en termes d'expertise. Quand vous parlez de comité aviseur, vous nous regardez puis vous vous dites — probablement, je ne veux pas vous mettre des mots dans la bouche — que l'expertise n'est pas suffisante à l'État, actuellement.

M. Lavoie (Alain) : Vas-y, Nicole, mais je pense qu'on va répondre la même chose.

Mme Martel (Nicole) : Oui. Bien, moi, je dirais, le mot-clé de ces temps-ci, c'est diversité, diversité d'opinions aussi, là, donc diversité de genres, de cultures et d'opinions. Comme je vous le mentionnais, on est toujours étonnés — je le sens encore au quotidien, ça fait quand même quelques années que je suis dans le milieu — des expertises locales que nous avons, qui travaillent avec des entités hautement sécuritaires ici ou ailleurs.

Donc, pourquoi se priver de ces cerveaux-là? C'est des gens qui n'ont pas d'intérêt mais qui pourraient participer à un comité aviseur simplement pour partager des bonnes pratiques. Je suis certaine que, dans les ministères, les différents ministères et organismes, il y a déjà des gens qui font de la veille, qui regardent ce qui passe dans certaines autres administrations, mais on pourrait l'avoir aussi à travers de gens qui formeraient un comité aviseur, par exemple. C'est toute la force aussi des conseils d'administration, quand on a un conseil d'administration diversifié. Donc, c'est une pratique qu'on recommanderait pour ce sujet aussi délicat que ça.

M. Barrette : O.K. Je reviens encore à la question que je vous avais posée tantôt, là. Je comprends que je vais vous poser peut-être une question qui peut vous mettre mal à l'aise, là, mais l'architecture de sécurité qui a été proposée, là, elle est cohérente avec les plus grands standards que vous voyez dans votre... il n'y a pas de... vous n'avez pas vu, là, vous n'avez pas entendu d'élément qui était discordant, d'une part? Et, d'autre part, il n'y a rien qui aurait été raté, là, ah, ils ont oublié de faire telle chose, ah, ils ont oublié tel...

M. Lavoie (Alain) : Écoutez, M. Barrette, un, on ne veut pas... comme je vous dis, là, vous pouvez avoir différentes opinions là-dessus, à savoir, hier, j'entendais : centraliser versus décentraliser. On n'est pas des experts, nous, mais ce que je peux vous dire, c'est que je vois les deux modèles. Quand on parle des «blockchains», c'est un mouvement décentralisé, quand on... puis on a le mouvement centralisé, mais, en même temps, tu peux avoir le mouvement... Je

vous dirais, à ce niveau-ci, O.K., on ne peut pas juger, en tout cas, nous, de notre côté. Je ne pense pas avoir la compétence de juger correctement. Dans les... Quand on... si on tombe dans les entrailles, là, puis on va voir dans les détails, peut-être qu'on pourra juger, mais je pense que le gouvernement est très bien équipé pour pouvoir prendre les bonnes décisions puis qu'il y a de la compétence pour le faire, ou, sinon, va aller la chercher, mais je ne pourrais pas dire, là.

On a très peu d'information pour pouvoir dire : à gauche ou à droite, mais ce que je peux dire, quand on dit centraliser versus décentraliser, bien, il y a des mouvements différents qu'on voit dans le... on a le mouvement centralisé, puis il y a le mouvement décentralisé, qui est, par exemple, avec les «blockchains». On décentralise pour assurer que... avec toute une probité des choses. Mais, ceci dit, je pense qu'il ne faut pas mélanger ces choses-là, puis on n'est pas des experts dans ce sens-là, M. Barrette, c'est tout.

M. Barrette : Êtes-vous des experts en chaîne de blocs?

M. Lavoie (Alain) : Écoutez, j'ai implanté ça chez nous, là, mais pas... j'ai implanté ça, on a ça dans nos technologies, mais je ne veux pas... il y a des gens meilleurs que moi là-dedans, puis l'acuité, on ne vient pas se positionner comme des experts, on vient se positionner pour donner les besoins de l'industrie puis ces choses-là.

M. Barrette : O.K. Pouvez-vous... Là, il me reste à peu près 30 secondes, là. J'aurais eu envie de vous demander d'élaborer, mais je n'aurai pas le temps, là, sur au moins un «big picture» d'équipe aviseur et de direction, mais on n'aura pas le temps de regarder ça, il ne me reste pas assez de temps. Alors, je vous remercie d'être venu aujourd'hui nous entretenir. Je pense que ça a été bien utile et bien intéressant. Merci beaucoup.

Le Président (M. Simard) : Je cède maintenant la parole au député de Rosemont.

M. Marissal : Merci, M. le Président. Chers collègues, M. le ministre, il me semble qu'on s'est vus il n'y a pas très longtemps, là. Je n'arrive pas à me souvenir où. Mme Martel, M. Lavoie, c'est toujours un plaisir de vous revoir, même si c'est virtuel.

Le ministre... et le projet de loi, là, qu'on décode, là, qu'on est en train de découvrir, essentiellement, on nous dit : Ça touche essentiellement et même, je dirais, exclusivement, la circulation de données personnelles dans la bulle, dans le giron gouvernemental, autrement dit, entre ministères et peut-être entre certains départements, agences, là, Revenu, par exemple, on peut imaginer. Pourtant, depuis hier, là, qu'on a commencé ces auditions-là, il y a beaucoup de gens qui nous amènent systématiquement hors du giron gouvernemental ou de la machine pour s'approcher toujours bien, bien proche du privé, un petit peu sur la pointe des pieds, d'ailleurs, sans trop vouloir le dire.

Vous, en voyez-vous un, lien entre 95 et ce que vous avez nommé tout à l'heure, Mme Martel, la relation entre l'État et le secteur privé?

Mme Martel (Nicole) : Le seul lien que je fais automatiquement, c'est que... ce que je comprends, c'est que le p.l. n° 95 vient encadrer, vient donner un cadre de gestion pour la transformation numérique qui va être au service des citoyens et des entreprises. Puis j'aimais l'exemple, je pense, qui était donné hier : si quelqu'un a besoin de son certificat de naissance, il n'a peut-être pas besoin de se rendre sur la rue Saint-Urbain pour aller chercher la dernière copie, faire la ligne, après ça, l'amener au ministère, et tout ça, si on sait, là... Nous, on travaille avec le gouvernement du Québec, on sait que l'information est détenue, bien, peut-être que vous pouvez aller la chercher là-bas. Donc, c'est le lien que je ferais avec le privé.

Puis là, bien, je vois énormément de bénéfices pour les entreprises. Quand on parle du fameux «red tape» pour les entreprises, si ça peut éliminer de ces irritants-là, bien, c'est souhaitable qu'on ait, bon, la permission de transférer ou d'échanger des données entre les ministères et organismes. Donc, ça, c'est le lien le plus immédiat que je ferais au bénéfice du privé.

M. Marissal : Bien là, on va s'entendre, là, je pense que personne n'aime ça, se prendre les pieds dans le «red tape», là. On a tous et toutes vécu des expériences où on nous demandait d'envoyer une photocopie de notre passeport à l'Agence du revenu du Québec parce qu'il y avait une faute dans notre nom, là, ou une faute dans la date de naissance, ce qui m'était déjà arrivé il y a quelques années, ça, on va s'entendre là-dessus. Puis c'est vrai qu'une entreprise doit aussi transiger avec le gouvernement. Personne ne souhaite que ça prenne quatre jours juste pour trouver la bonne personne. Des histoires d'horreur, il y en a, il y en a, il y en a. Ça fait quand même 30 ans, là, que je couvre ça, j'en ai entendu.

Mais moi, ce n'était pas de ça dont je parlais, et je pense que vous le savez. Moi, je parle de cette nouvelle ressource naturelle qu'on appelle les données personnelles, et vous êtes là-dedans aussi. Il se trouve que, depuis hier, on a entendu parler du Scientifique en chef du Québec qui a donné un mandat à la Commission d'éthique en science et en technologie pour étudier cette relation entre l'État et, éventuellement, le privé, les fondations de recherche... les Fonds de recherche du Québec. Tout est lié, là. Je présume que vous êtes aussi dans cette mouvance, là, et vos membres le sont aussi.

M. Lavoie (Alain) : Oui. M. Marissal, écoutez, moi, je suis aussi très impliqué dans l'écosystème de l'IA puis je suis très, très, très, aussi, préoccupé par tout ce qui est au niveau de mettre des entrepôts de données, rendre ça accessible, puis je veux que ça soit fait comme il faut, si c'est fait, là. Un jour, si c'est fait de quelque façon que ce

soit, il faut que ça soit fait comme il faut, parce que ça va avoir une incidence importante sur le monde de l'intelligence artificielle par la suite, au Québec, c'est-à-dire...

Le Président (M. Simard) : En conclusion.

M. Lavoie (Alain) : Et donc, dans ce contexte-là, je vous dirais qu'il reste encore des choses à faire par rapport à ça, puis on va suivre les dossiers de près. Et c'est pour ça qu'on dit : p.l. n° 14, p.l. n° 64, p.l. n° 95 puis peut-être d'autres p.l., éventuellement, vont venir. On est en train de construire... M. le ministre est en train de construire un avion, puis on suit ça de très près, puis on veut que ça soit bien géré, les données, quelle que soit l'organisation, quelles que soient...

Le Président (M. Simard) : Très bien.

M. Lavoie (Alain) : ...les personnes qui la gèrent. Merci.

M. Marissal : ...autant de la destination que de l'appareil, ce pour quoi je vous posais cette question. Merci.

Le Président (M. Simard) : Merci. Alors, Mme Martel, M. Lavoie, de l'Association québécoise des technologies, merci beaucoup pour votre présence parmi nous ce matin. Ce fut fort agréable.

Et, compte tenu de l'heure, nous allons ajourner nos travaux jusqu'à 14 h 30. À plus tard.

(Suspension de la séance à 12 h 20)

(Reprise à 14 h 37)

Le Président (M. Simard) : Alors, chers collègues, en direct de la salle La Fontaine à l'Assemblée nationale, nous reprenons nos travaux.

Vous savez que notre commission est réunie virtuellement afin de procéder aux consultations particulières et aux auditions publiques sur le projet de loi n° 95, Loi modifiant la Loi sur la gouvernance et la gestion des ressources informationnelles des organismes publics et des entreprises du gouvernement et d'autres dispositions législatives.

Alors, sur ce, nous recevons la présence de M. Claude Sarrazin, spécialiste en cybersécurité. M. Sarrazin, je sais que vous êtes un habitué. Bienvenue parmi nous.

M. Sarrazin (Claude A.) : Merci beaucoup.

Le Président (M. Simard) : Vous savez que vous disposez de 10 minutes pour faire votre présentation.

M. Claude A. Sarrazin

M. Sarrazin (Claude A.) : Oui. Bien, tout d'abord, je voudrais vous remercier pour m'avoir invité de participer aux travaux de la commission. J'ai lu avec intérêt le projet de loi. Ça a été bien pensé. C'est un exercice qui était intéressant. Toutefois, je dois vous aviser que je n'ai pas... Malheureusement, par respect, je dois vous dire que je n'ai pas déposé de mémoire. Le délai entre ma convocation et ma présence devant vous ne me permettait pas, je pense, de présenter un document qui aurait été valable. Donc, c'est ça.

Également, l'autre point qu'il est important de comprendre, c'est que, oui, je fais de la cybersécurité, j'oeuvre dans le domaine des enquêtes maintenant depuis 30 ans. J'ai fait énormément d'enquêtes dans le domaine du vol de données et j'ai enseigné également, à l'UQAM, ce que j'aimais appeler le volet cybercrimes à l'École des sciences de la gestion, à la maîtrise. Ça fait que, donc... mais je ne suis pas un expert en informatique. Je ne vends pas de logiciel, je n'en recommande pas, ce n'est pas là mon objectif principal. Ça fait que, donc, si tout le monde comprend bien ça, surtout pour la période des questions... Et ce que je vais faire, c'est qu'à la suite de mon témoignage je me permettrai de vous envoyer un document qui reprendra les principaux points, là, de ma présentation aujourd'hui.

Donc, la réalité aujourd'hui est que peu ou pas de données ne sont désirables aux yeux des cybercriminels. Que ce soient des attaques visant les systèmes eux-mêmes ou visant les données qu'ils détiennent, la réponse à ces enjeux est généralement de mettre en place différentes barrières concentriques pour contrôler l'accès aux données ou par différentes formes de ségrégation et de cryptage des données elles-mêmes. Donc, on va essayer de protéger l'environnement, le système ou la donnée que contient cet environnement-là. Souvent, ça va être un échantillonnage des deux mesures. Toutefois, le problème ne s'arrête pas là.

• *(14 h 40)* •

Je vais vous donner l'exemple d'opération EMMA 95. Dans ce cas-ci, les services de police européens, principalement la France, la Grande-Bretagne et les Pays-Bas, ont monté une opération pour attaquer les serveurs d'une firme appelée EncroChat. EncroChat était un outil de communication utilisé par les criminels de tout type, de tout acabit, principalement en Europe, mais notamment en Amérique du Nord également, qui était hautement sécurisé. Ça fait que, donc, on parle avec des protocoles d'«encryption» très sévères, très difficiles d'accéder à l'information.

Et, même si on connaissait l'existence de ça, il n'y avait pas moyen de pénétrer le système, le réseau. Et, malgré cette sécurité importante là, les autorités ont réussi à déjouer ces mesures en insérant tout simplement, à partir d'un des serveurs d'EncroChat, un «update» qui contenait ni plus ni loin un malware, donc une... Et je m'excuse pour les anglicismes, c'est terrible dans le domaine de l'informatique. Et ils ont attaqué, de cette façon-là, l'entièreté des 50 000 utilisateurs d'EncroChat, O.K.?

Je donne cet exemple-là du côté policier, ce qui peut sembler bizarre un peu, mais c'est parce que c'est très bien documenté, ce qui est plutôt rare quand on fait affaire avec des hackers. Donc, à partir de ce moment-là, ils ont... ça leur a permis d'identifier, tout simplement, les utilisateurs, les identités de ces personnes-là et les localités où ils se trouvaient, tout simplement en utilisant les tours de cellulaires qui étaient à proximité des appareils qui étaient connectés à EncroChat. Par la suite, bien entendu, bien là, ils ont intercepté les communications à travers le serveur dédié, qui était également... qui était situé en territoire français, pour la petite histoire. Et, à partir de ce moment-là, ils ont réussi à craquer l'ensemble du réseau et du système, qui était quand même assez lourdement protégé. En temps réel, les policiers ont obtenu, donc, les communications de tous ces criminels-là.

Le résultat final, puis on peut juste en être heureux, il y a eu au-dessus de 1 000 arrestations, à date, on a 100 millions d'euros d'argent, de drogue et d'armes qui ont été saisis, et puis on s'en réjouit. Mais toutefois, si la police a eu la capacité technique de faire ce travail, ne pensez-vous pas que les criminels, eux aussi, ont cette capacité? La réponse, bien entendu, c'est oui.

Ça fait que, donc, ce que ça nous apprend, cette histoire-là, puis je m'excuse si je suis un peu anecdotique, mais c'est vraiment qu'il n'y a pas de système d'«encryption», il n'y a pas de système de sécurité, peu importe sa valeur, qui va nous protéger contre toutes les menaces. Alors donc, comment nous prévenir de ce type d'attaque? On doit diversifier nos méthodes de protection en alliant les principes de sécurité concentrée, mais également en développant la capacité de voir venir les menaces. Et cet aspect doit être développé d'un point de vue humain en développant l'expertise et en se concentrant non pas sur la menace immédiate, ou sur un type de défense statique, ou une suite de logiciels inviolables, comme c'est souvent le cas, comme dans le cas d'EncroChat, mais sur des équipes multidisciplinaires qui ont l'agilité de pouvoir rapidement mettre en oeuvre les outils appropriés pour répondre à ces risques bien réels.

Et ça, c'est sans parler du facteur humain, parce que, bien entendu, et on l'a vu dans une multitude de cas présentement, récemment, c'est souvent le facteur humain qui vient nuire à tout l'ensemble de la protection des données, que ça soit au point de vue réseau ou que ça soit les données portables, peu importe. Ça fait que, donc, dans le facteur humain, on a les utilisateurs des systèmes eux-mêmes qui deviennent porteurs des vulnérabilités inhérentes à l'utilisation journalière, que ça soit un employé, que ça soit un sous-traitant, que ça soit une personne qui est autorisée à accéder l'information d'une façon ou d'une autre.

Et ça, c'est d'autant plus dommageable que ça affecte la confiance directe des utilisateurs dans ces systèmes-là. On le voit souvent, la confiance des gens a été atteinte. Je ne pense pas qu'il n'y a pas personne parmi vous qui n'a pas subi une perte de données dans les trois dernières années. Je peux vous dire, pour ma part, que moi, ça m'est arrivé à trois fois dans diverses institutions, dans divers organismes. C'est une réalité. Ça fait que, donc, comment qu'on fait... et c'est essentiel.

Là, on parle d'une entreprise privée, d'organismes privés, mais là on parle de L'État. L'information détenue par l'État est d'une importance capitale, ne serait-ce que pour la confiance des citoyens par rapport à l'État. Ça fait que, donc, on se retrouve dans une situation où... Et la question qu'on doit se poser, c'est : Qui doit détenir quelle information? Et est-ce qu'on doit détenir toute l'information tout le temps? Est-ce que c'est nécessaire d'avoir cette masse critique d'informations là? Parce que veux veux pas... puis on va revenir au facteur humain après, mais, veux veux pas, plus on a d'informations regroupées de façon centralisée, plus on devient vulnérables à des attaques potentielles. Parce que c'est la règle de la menace et du risque, là, à partir de ce moment-là, on devient une cible intéressante. Et, comme je disais au début, il n'y a pas d'information qui n'est pas recherchée par les cybercriminels, à toutes sortes de fins.

Et tout ça m'amène à aussi, également, approcher au point de vue de la transparence. Une des choses que j'enseigne à mes étudiants en matière de cybersécurité, c'est la nécessité de transmettre l'information sur la nature de nos infrastructures, même au point de vue des organismes gouvernementaux, même le processus d'appel d'offres. Est-ce qu'on est obligés d'avoir le même niveau de transparence? Et je peux comprendre vos appréhensions par rapport à la valeur des contrats, et etc., mais, à partir du moment qu'on télégraphie le type de logiciel qu'on utilise, le type d'infrastructure qu'on utilise, les outils informatiques qu'on utilise, et que c'est accessible par un clic de souris parce que c'est des contrats publics, on vient de fournir à des criminels toute l'information dont ils ont besoin pour pouvoir attaquer ces mêmes réseaux là. Ça nous rend excessivement vulnérables, mais, en même temps, on a une règle d'éthique, au point de vue des dépenses gouvernementales, qui vient nous attacher. Ça fait que ça, c'est une complexité accrue dans votre position.

Alors donc, si on regarde, toujours du côté humain, je vais vous revenir... et là j'ai complètement parti de mon texte, vous m'excuserez. Je vais vous donner un autre exemple où je suis intervenu directement dans un mandat de vol de données dites protégées, dans une infrastructure ayant la cote STC, donc très secret, compartimenté, qui est la plus haute cote en matière de sécurité nationale. Donc...

Le Président (M. Simard) : Peut-être en conclusion?

M. Sarrazin (Claude A.) : Oui, je vais arriver rapidement. Dans ça...

M. Caire : M. le Président?

Le Président (M. Simard) : Oui?

M. Caire : Si M. Sarrazin veut continuer sur le temps de... sur mon temps, il n'y a pas de problème.

Le Président (M. Simard) : Parfait.

M. Caire : Je vais le laisser finir sa présentation. Je pense que c'est le moins qu'on puisse faire pour lui.

Le Président (M. Simard) : Alors, allez-y, M. Sarrazin. Vous auriez jusqu'à 16 minutes à vous tout seul encore.

M. Sarrazin (Claude A.) : Bon, bien, excellent, merci, c'est très apprécié de votre part. Donc, on se retrouve dans un environnement qui est hypersécurisé. Il y a des traces comme quoi que l'information a été... s'est retrouvée à l'externe de cet environnement sécurisé là. Les analystes en sécurité des TI de l'organisation en question, majoritairement des ingénieurs bien meilleurs que moi en informatique, je vous le dis tout de suite, font des analyses et ne retrouvent aucune trace de possibilité d'extraction ou de sortie des données, et on parle de plusieurs milliers de pages de documents.

On fait enquête, et ce qu'on a trouvé, et on parle d'une organisation qui dépense des dizaines de millions de dollars, annuellement, en sécurité des TI, là, ce qu'on a trouvé, c'est qu'un employé autorisé à accéder l'information, donc il n'accédait pas de l'information à laquelle il ne devait pas avoir accès, a tout simplement utilisé une caméra 35 mm jetable qu'il portait sur lui pour photographier, parce qu'il ne pouvait pas utiliser son téléphone cellulaire, les téléphones cellulaires, dans l'enceinte où il se trouvait, étaient interdits, et il devait passer un portique détecteur de métal pour pouvoir rentrer à l'intérieur. Ça fait qu'il utilisait une caméra 35 mm jetable, qui est faite en plastique et en carton, pour votre information, avec quelques ressorts, très peu de pièces métalliques. Il passait à travers le portique de détection facilement avec ça. Il prenait les photos et, après ça, il y avait quelqu'un qui reprenait à partir des photos 35 mm et les retranscrivait tout simplement dans des nouveaux documents informatiques pour pouvoir les partager avec les personnes qui voulaient acquérir cette information-là.

• *(14 h 50)* •

Ça fait que, donc, il n'y en a pas, de mesure de sécurité de l'information qui peut protéger contre un comportement semblable. Là, on est dans du humain pur, ça fait que ça devient particulièrement difficile pour toute organisation. On peut faire de notre mieux, et c'est ce que j'espère que nos représentants vont faire dans ce cas-ci. Je pense que la base même du projet est intéressante.

J'ai huit points qui, je crois, sont essentiels à la sécurité de l'information de l'État. En premier lieu, c'est l'aspect prévention. En deuxième lieu, puis je vais réduire pour moins couper de temps, en deuxième lieu, je vois la mitigation des risques, donc essayer, justement, de réduire ces risques-là. Est-ce qu'on a besoin de cette information? La formation en situation réelle, non pas assis sur une chaise à écouter un professeur, mais bien d'avoir de la formation en temps réel dans des situations concrètes, un peu comme certaines organisations. Puis je ne veux pas nommer d'organisations, nécessairement, mais il y a différentes organisations qui utilisent des espèces de cybergym où est-ce qu'on se retrouve à être en conflit direct, et là on voit des attaques en temps réel.

La diversité des équipes pour éviter des modèles trop linéaires, qui est superimportant. Ils nécessitent non seulement des gens en technologie de l'information, mais des gens en ressources humaines, des gens en enquête, des gens en protection pour que tous ces groupes-là puissent se parler ensemble, parce qu'il n'y a pas une solution unique à ces problématiques-là. La diversité des équipes, bien entendu, la séparation des fonctions... Ça fait que... Donc, qu'on ait quelqu'un responsable de la sécurité de l'information, c'est une chose, mais, quand il y a une fuite d'informations, l'enquête liée à cette fuite-là doit être séparée. On ne doit pas être consanguin quand on fait l'enquête pour déterminer qui est responsable. Et si, effectivement, il y a eu des erreurs de commises, bien, il faut pouvoir les identifier.

La validation des mesures et des politiques. Les enquêtes sur les événements par des tiers, ça peut être d'autres organismes, ça peut être d'autres ministères, mais il faut... ou une unité centralisée, mais ça prend des gens qui ne sont pas partie eux-mêmes à la prise de décisions sur les mesures de sécurité. Puis définir des limites de temps pour déclaration des incidents et pour effectuer l'enquête pour obliger et structurer cette situation-là, on l'a déjà au fédéral. Et nous devrions évaluer notre besoin de conservation des informations. Qu'est-ce qui est essentiel au fonctionnement de l'État? Qu'est-ce qui est accessoire? Et qu'est-ce qu'on a besoin, mais qu'à un très court terme? Je vous dirais que c'est mes huit points les plus importants, je vous dirais, et c'est autour de ça que ça s'oriente. Je vous remercie.

Le Président (M. Simard) : Merci, M. Sarrazin. Merci. Alors, je cède la parole au ministre qui dispose de 11 min 40 s.

M. Caire : Merci, M. le Président. Merci, M. Sarrazin. Je vais avoir quelques petites questions. En premier lieu, sur le projet de loi n° 95, je comprends... puis peut-être vous entendre succinctement là-dessus, je comprends que d'avoir un chef gouvernemental de la sécurité de l'information, un chef de la transformation numérique, un gestionnaire de la donnée, donc, des fonctions qui seront appelées à occuper différentes responsabilités, ce volet-là, cette gouvernance-là de la sécurité et de la sécurité de l'information, c'est quelque chose qui vous plaît. Est-ce que j'ai bien compris ce que vous avez dit?

M. Sarrazin (Claude A.) : Oui, tout à fait, c'est une... ça rentre tout à fait dans cet esprit-là. Je rajouterais à ça une notion d'indépendance dans l'enquête et la validation. Ça fait que, donc, c'est le seul aspect, oui.

M. Caire : Oui, mais ça, on irait plutôt du côté de la Commission d'accès à l'information, de toute façon. Donc, cette indépendance-là, elle est assurée.

J'aimerais vous entendre aussi sur la notion de hub, parce que vous avez parlé de... bien, de hub, je vous dirais que c'est le Pr Gambs qui nous a amené cette notion-là. Moi, je parle de sources de données, parce qu'actuellement la façon dont on conserve la donnée, c'est qu'on a 300 organismes, bon an mal an, au gouvernement du Québec, qui collectent tous l'ensemble des informations dont ils ont besoin pour leurs prestations de services. Donc, on surmultiplie les banques de données, qui sont relativement complètes, sur chaque citoyen. Ma prétention, c'est que ça, ça surmultiplie aussi les risques de fuites ou d'attaques informatiques. L'autre extrémité, ce serait, comme Pr Gambs disait, puis je ne sais pas si vous avez entendu son témoignage, de tout centraliser dans une même banque, qui n'est pas mieux, parce qu'en cas de réussite d'une attaque, bien là, on a accès à l'ensemble du plat de bonbons.

Ce qu'on préconise, le gouvernement du Québec, c'est de fonctionner un peu comme un modèle relationnel. Je sais que vous avez dit que vous n'étiez pas informaticien, donc je vais y aller avec peut-être un concept plus compréhensible, mais c'est de dire : différentes sources de données officielles, mais spécifiques à des profils de données, comme santé, éducation, état civil, revenu, famille, etc., donc autant de sources de données. Donc, il y a une division, un éclatement de l'information, mais il n'y a pas une surmultiplication, donc 300 versions différentes ou 300 versions étalées dans 300... ou sites différents, d'un même individu. J'aimerais vous entendre sur ce modèle-là, si vous pensez qu'on est... En matière d'accès, mais aussi en matière de protection, si ça peut nous amener une configuration intéressante au niveau de la sécurité.

M. Sarrazin (Claude A.) : Ça peut être intéressant, en autant que le niveau de sécurité n'est pas modifié en fonction de la nature de l'organisation qui accède ou du niveau de sécurité de l'organisation qui accède à ces bases de données là. Donc, ça fait que, oui, je suis d'accord avec vous, j'aime mieux ce concept-là que le concept d'un hub centralisé où tous les organismes se connectent et vont chercher l'information à leur guise. Parce qu'effectivement ça peut constituer un risque plus important, parce que ça vient relever la menace, automatiquement. Ça fait que, donc, on est dans un endroit où est-ce que, oui, ça pourrait être plus confortable de le faire de cette façon-là. Maintenant, il faut voir... il faut le maintenir.

Il y a un organisme fédéral qui avait un peu le même modèle qu'ils ont utilisé, sauf qu'eux ont mis des niveaux de sécurité qui étaient différents selon la nature des opérations. Donc, pour donner l'exemple, quand il y a eu infiltration, un petit poste de la Saskatchewan était sur le même réseau, finalement, qu'une unité importante à Montréal. Et, à partir de ce moment-là, quand l'infiltration, le «hack», s'est fait, ils sont rentrés par le petit poste qui avait moins de... Ça fait que, donc, c'est juste à ce niveau-là qu'il faut avoir une certaine prudence. Sinon, pour le reste, le concept est excellent. Ultimement, on verra ce que l'avenir nous réserve. Gardez en tête que c'est... D'ici 10 ans, on va avoir le «quantum computing», ça fait que... l'informatique quantique qui va venir changer la donne totalement quant à nos mesures de sécurité. Ça fait que, donc, il y a un bref espace...

M. Caire : Qui va venir changer la donne au niveau de la performance des systèmes, mais sur la façon de se protéger... En tout cas, je ne veux pas anticiper ce que l'informatique quantique va nous amener, comme l'intelligence artificielle, mais vous pensez vraiment que ça va changer... Je donne un exemple, parce que je pense que ce que vous amenez comme élément, c'est important, de ne pas protéger la donnée, dans le fond, en fonction de qui l'utilise, mais de protéger la donnée en fonction de sa valeur et de sa sensibilité. Ça, j'ai cette prétention-là, mais, une chose à la fois, on va commencer par 95. Mais, dans le fond, ce que vous dites, c'est un peu ça, c'est qu'il faut qu'on s'assure d'avoir une protection de la donnée qui est proportionnelle à sa valeur et non pas de savoir est-ce que c'est Santé ou un tribunal administratif qui l'utilise. C'est un peu ça que vous dites?

M. Sarrazin (Claude A.) : Tout à fait, tout à fait. Puis ce que l'informatique quantique va venir changer, c'est que les capacités des systèmes, tels qu'ils sont présentement, permettraient de briser la majorité des codes qu'on utilise. Bon, il y en a certains... c'est discuté présentement, mais l'encryption même des données devient, effectivement, très vulnérable, là, plus on avance, là.

M. Caire : Mais, par contre, on peut peut-être imaginer que ces ordinateurs-là auront la puissance aussi de mettre en place des contremesures, mais ça, je ne me lancerai pas dans la futurologie...

M. Sarrazin (Claude A.) : Mais l'encryption quantique existe présentement... Excusez-moi, M. Caire, mais l'encryption...

M. Caire : Oui, oui, oui. Non, mais dans le sens... Je ne suis pas un spécialiste, là, ce n'est pas... Vous avez amené un élément qui a retenu beaucoup mon attention puis sur lequel je voudrais vous entendre. Vous avez parlé de cybergyms, donc vraiment des centres d'entraînement en situation réelle. En quoi, ça, ça se distingue des simulations qu'on peut faire en milieu de travail? Comment ça fonctionne exactement ces... les cybergyms?

• *(15 heures)* •

M. Sarrazin (Claude A.) : C'est le rythme, c'est des attaques en temps réel. Ça fait que, donc, les gens sont soumis à la pression d'une attaque réelle par rapport à des systèmes, des infrastructures, des mécanismes, et donc... parce que leur modèle est reproduit à l'intérieur même de cet environnement-là.

M. Caire : O.K. Donc, on reproduit la structure de l'organisation à protéger, mais en milieu contrôlé, j'imagine.

M. Sarrazin (Claude A.) : Exact. Tout à fait, c'est en milieu...

M. Caire : Et donc on attaque les gens en leur disant : Bien, voilà... En fait, c'est, genre, les équipes bleues, les équipes rouges, là, qu'on voit dans les «hackfests».

M. Sarrazin (Claude A.) : Oui, c'est ça, exactement, selon le même principe, oui, tout à fait.

M. Caire : O.K. Puis ça, ça existe au Québec, ces lieux d'entraînement là?

M. Sarrazin (Claude A.) : Pas présentement, à ma connaissance. Il y en a à New York, il y en a... il y a différentes organisations québécoises qui ont regardé ce... j'ai fait une visite à New York dans un environnement comme ça puis je sais qu'il y a des gens d'autres organismes de l'État qui étaient présents, eux aussi, pour aller voir comment ça se passait, voir l'efficacité de la formation. Ça a été développé, dans ce cas-ci, en Israël. Ça fait que, donc, c'est des systèmes... C'est ça, exactement.

M. Caire : Pourquoi je ne suis pas surpris?

M. Sarrazin (Claude A.) : Oui, c'est ça, tout à fait.

M. Caire : Vous avez amené un élément, puis je veux vous entendre là-dessus aussi, au niveau des enquêtes, lorsqu'il y a un incident de confidentialité ou une fuite de données. Vous avez dit : Ce serait intéressant qu'il y ait une limite de temps à la divulgation et une limite de temps à l'enquête. J'aimerais vous entendre là-dessus parce que c'est une notion dont on a discuté, je vous dirais, sur un autre projet de loi, et pour laquelle on se disait : Bien, écoutez, il y a des enquêtes... Puis on a un exemple récent, au Québec, là, d'une enquête pour un événement qui s'est produit il y a maintenant quelques années, et l'enquête est toujours en cours, en tout cas, de ce qu'on en sait.

Comment on peut mettre ces limites de temps là, sur quelles bases on peut les fixer, et pourquoi c'est intéressant de fixer une limite de temps?

M. Sarrazin (Claude A.) : Bien, un, c'est que ça oblige les organisations à passer de l'avant et donc à passer à l'action rapidement. Ça fait que, donc, il y a un peu... ça laisse moins de temps un peu aux gens de pouvoir se décharger de leurs responsabilités, ça leur oblige à prendre action rapidement, ça oblige à mettre en place des structures pour pouvoir répondre à ça et ça enchâsse, ça permet d'avoir un guide un peu de qu'est-ce qu'on va accepter.

C'est sûr que ça peut être beaucoup plus long, et vous le savez, on l'a vu, une enquête, ça peut être très long. Je l'ai fait, moi-même, pour le Tribunal pénal international. Ça fait que, donc, oui, on part avec un délai de trois mois. Dans le cas d'un vol de données, ça nous a pris sept mois, environ, pour compléter l'enquête, et, après ça, on a déposé nos accusations, mais, initialement, être enchâssé dans une période de trois mois pour effectuer l'enquête, ça nous permet de mettre en place les protocoles.

Et c'est bizarre à dire, mais, l'être humain étant ce qu'il est, bon, bien, parfois, on a tendance, et je l'ai souvent vu dans des organisations, à remettre à demain ce qui pourrait être fait aujourd'hui. En ayant des contraintes de cette nature-là, bien là, ça oblige les gens à procéder parce qu'ils savent qu'ils ont une responsabilité par rapport à la loi. Ça fait que, donc, je pense que ça ne peut pas nuire, au contraire.

M. Caire : Mon temps file, j'ai une petite dernière question. Mais est-ce que vous n'avez pas peur d'avoir l'effet pervers, c'est-à-dire de voir une enquête être bâclée, justement, parce que, là, on a cette contrainte de temps, puis il faut livrer quelque chose rapidement, puis on ne va peut-être pas au fond des choses, on passe par-dessus quelque chose qui va nous échapper puis qui aurait pu nous amener vers une piste où il y a plus encore que ce qu'on a vraiment trouvé?

M. Sarrazin (Claude A.) : Oui, absolument, et c'est pour ça que, dans les lois ou les règlements, ce qu'on veut introduire, c'est une notion de... quand l'enquête se poursuit, bien, à ce moment-là, on peut prolonger ce délai-là, mais il faut juste... L'enquête initiale doit être initiée en tant de délai, il y a telle période pour pouvoir enquêter, et, après ça, bien, c'est... quand on sait qu'on s'en va vers une solution, bien là, on peut procéder. Ça fait qu'il faut démontrer qu'on a des résultats, qu'on a avancé, qu'il y a matière à poursuivre l'enquête, et c'est toujours l'idée d'avoir le maximum d'intervenants au dossier...

M. Caire : L'obligation de commencer.

M. Sarrazin (Claude A.) : L'obligation, c'est ça, exactement.

M. Caire : Je vois le président qui va nous interrompre. Donc, je vous remercie infiniment, M. Sarrazin, ça a été vraiment très agréable.

Le Président (M. Simard) : Vous lisez dans mes pensées, cher collègue. Je cède maintenant la parole au député de La Pinière.

M. Barrette : Bonjour, M. Sarrazin.

M. Sarrazin (Claude A.) : Bonjour.

M. Barrette : Je suis convaincu que ce n'était pas votre intention, mais vous nous avez fait peur.

M. Sarrazin (Claude A.) : On me reproche ça à l'occasion.

M. Barrette : Et ce n'est pas un reproche. Je vais vous avouer que, disons, que... Est-ce que vous voulez divulguer comment vous l'avez trouvée, ma...

M. Sarrazin (Claude A.) : Bien, écoutez, à force d'enquête. Et là on est sortis du milieu de l'enquête informatique, on s'est dit : Si l'information est sortie, ils ont trouvé une façon de la sortir, et on a utilisé des méthodes d'enquête traditionnelles, et on a trouvé l'information en faisant une perquisition à l'intérieur de la résidence du sujet, et là on a retrouvé les images qui avaient été converties en photos, puis etc. Ça fait que c'est... quand même, c'est du travail, mais, d'un point de vue informatique, et les gens avaient raison là-bas, tout était parfait, il n'y avait aucun problème.

M. Barrette : Eh bien! Non, c'est assez épeurant quand on pense à ça. Je vais continuer dans la suite du dernier bout de conversation que vous avez eu, là, en vous posant deux questions. Une des choses qui m'effraient dans ce que vous nous dites... je vais vous avouer qu'il y a certains niveaux de complexité que je n'avais pas soupçonnés. Une organisation parfaite peut se faire hacker, bon, fin de la discussion, vous en êtes la preuve vivante, bon, et par l'expérience. Est-ce qu'il y a... Il y a deux éléments que je veux aborder. Est-ce que la sécurité est plus dépendante de technologies que de protocoles?

M. Sarrazin (Claude A.) : Ça dépend. Ça dépend des organisations. Présentement, je vous dirais que la majorité des organisations sont plus dépendantes de la technologie que des protocoles. Les protocoles prennent du mieux, mais encore faut-il qu'ils soient respectés.

Il y a tellement de vulnérabilité, je pourrais vous en parler pendant des heures, mais je vais vous donner un simple exemple, O.K.? On a fait un dossier, aux États-Unis, dans le cadre d'un vol d'information et d'un vol monétaire importants. La personne qui a été impliquée là-dedans s'est fait voler son identité tout simplement parce qu'elle utilisait le e-mail de son organisation et également le même mot de passe que son organisation pour accéder à ses courriels dans tous ses comptes, y compris les médias sociaux. Tu sais, c'est une règle de base, en matière de sécurité de l'information, mais ça, tu ne peux pas prévenir contre un facteur humain de cette nature-là. Et les gens, tout ce qu'ils ont fait, c'est qu'il y a eu un hack dans un des sites de médias sociaux que la personne utilisait, ils ont récupéré ça, ils l'ont essayé, ça a fonctionné, ils ont eu accès au réseau informatique par la suite de façon légitime. Ce n'est pas bien, bien sorcier. C'est une règle de sécurité de base, quand même, qu'on connaît. Il y a beaucoup de gens qui font ça, vous seriez surpris de voir le nombre de personnes. J'ai vu des statistiques passer, à un moment donné, on parlait, dans le monde, de 23 millions de personnes qui reconnaissaient avoir cette pratique-là, d'utiliser un identifiant, un mot de passe pour tous leurs comptes.

M. Barrette : O.K., mais la technologie comme telle, elle doit avoir quand même son importance?

M. Sarrazin (Claude A.) : Absolument, absolument. C'est l'aspect concentrique de la sécurité.

M. Barrette : L'aspect concentrique?

M. Sarrazin (Claude A.) : Oui.

M. Barrette : O.K. L'autre élément que je voulais aborder, parce que ça, c'est la fin de la conversation que vous avez eue avec le ministre, là, ça m'a beaucoup titillé, ça, tout le concept de garder les gens sur la pointe de leurs pieds, là, en les challengeant tout le temps, là, vos cybergend, puis tout ça, là. Ça, il doit y avoir un grand éventail de possibilités, là-dedans, mais ce que je comprends de ce que vous nous dites, c'est qu'il doit y avoir un minimum, là, dans le monde d'aujourd'hui.

• *(15 h 10)* •

M. Sarrazin (Claude A.) : Oui, absolument. Il faut que les gens sachent, de façon réaliste, qu'est-ce qui peut se passer, comment que ça peut arriver, c'est quoi les vulnérabilités réelles de leurs réseaux. Trop souvent, on va s'appuyer sur l'aspect technologique. C'est un peu, tu sais, ce que le vendeur nous a dit, là, ultimement, on a tendance à vouloir croire ce qu'on nous dit concernant la robustesse de certaines infrastructures informatiques. Malheureusement, si ces infrastructures-là ne sont pas maintenues à niveau, si on n'analyse pas bien nos menaces puis nos risques, bien, on se rend très vulnérable. Ça fait que, donc, oui, il y a une importance capitale à tous les niveaux.

Et je vous dirais que c'est l'ensemble de l'oeuvre qui compte, et non pas un élément seul. Pris individuellement, tous ces éléments-là font que vous êtes vulnérable. Si on les met tous ensemble, bien là, à ce moment-là, on réduit notre vulnérabilité. On ne devient pas invulnérable, on la réduit. Et c'est d'avoir ce confort-là de dire : Bon, bien, à ce niveau-là, je suis suffisamment confiant dans la protection des données.

M. Barrette : La raison pour laquelle je vous pose cette question-là... et ça ne met pas en cause le ministre actuel, qui est avec nous, M. Sarrazin, là, mais, vous savez, les gouvernements ont une fâcheuse tendance à faire des coupures dans les éléments qui ne sont pas les éléments les plus visibles, hein? Ça arrive, ça, que, ah bien, là, le budget, là, on n'arrivera pas cette année puis là, donc, on fait des coupures. En général, ce qui n'est pas visible, là, ça ne sera pas le serveur, ça va être le gars ou l'équipe qui, elle, fait ça à l'année longue. Ça veut dire que, dans la structure même du fonctionnement de l'entreprise qu'est l'État il peut y avoir des points d'achoppement, là. Vous, est-ce que vous nous dites, là, essentiellement : Une grosse compagnie ou un gouvernement qui ne se maintiendrait pas à jour pendant deux ans, obligatoirement, est très, très à risque?

M. Sarrazin (Claude A.) : Tout à fait, absolument. On ne peut pas baisser les bras, on ne peut pas dire : O.K., là, maintenant, je suis en sécurité, je n'ai plus besoin de m'en faire. Ça ne marchera pas. C'est comme... ça serait l'équivalent de faire la route entre Montréal et Québec, de conduire les yeux ouverts les 15 premières minutes, ça a bien été, puis, après ça, s'endormir en arrière du volant puis laisser rouler, bien entendu, quand vous n'avez pas de chauffeur, là, mais quand c'est vous qui conduisez... mais c'est exactement ça. Et là, en arrivant pas loin de Montréal, bien, je vais mettre mon réveil pour me réveiller, puis je vais continuer ma route, puis tout va bien aller. Ça n'arrivera pas, là.

M. Barrette : ...on connaît tous, maintenant, par les médias, le couple de personnes qui sont mortes au volant... pas au volant, mais assises dans une Tesla, où elles dormaient.

M. Sarrazin (Claude A.) : Oui, exact.

M. Barrette : Ce n'est pas parce qu'il y a un robot qui conduit que c'est sécuritaire.

Là, je ne sais pas, c'est vraiment une question de curiosité, là. Tantôt, je vous demandais si la technologie était... la sécurité était plus technologie dépendante que non, et puis je ne sais pas du tout si ça peut s'appliquer aux données massives, là, mais une technologie de chaîne de blocs, là, ça se hacke ou ça ne se hacke pas, de votre expérience?

M. Sarrazin (Claude A.) : Oui, il y a des méthodes qui existent pour pouvoir modifier le chaînon de la chaîne de blocs. Il y a eu des expériences dans le passé qui ont démontré que c'était possible. Maintenant, il y a eu des correctifs de mis en place, mais, ultimement, il n'y a rien qui ne se hacke pas, ultimement, parce que, si on a quelqu'un à l'interne, si on a quelqu'un qui est chez le fournisseur de logiciel, si on a quelqu'un qui est... n'importe où, le «man in the middle», finalement, là, qui a accès aux données, bien, à ce moment-là, il y a des possibilités, il y a différentes façons de le faire.

M. Barrette : O.K. Quand vous nous regardez au travers du projet de loi n° 95, est-ce que vous considérez qu'au moins on s'adresse à tous les éléments les plus pertinents en matière de sécurité?

M. Sarrazin (Claude A.) : Oui. Je crois que oui. Je pense que la réflexion qui a été faite jusqu'à présent est importante. Ça, ça ressort clairement du document que j'ai lu. Et, oui, la majorité des éléments sont démontrés là. Comme je vous disais, et bien humblement, il y a les quelques points que j'aimerais voir là-dessus, mais ce n'est pas moi qui vais le décider, c'est vous.

M. Barrette : Ce ne sera pas moi non plus, mais on va travailler fort... Bon, M. Sarrazin, je vous remercie, ça a été très, très utile.

M. le Président, si vous n'avez pas d'objection, moi, je pourrais faire un cadeau à mon collègue de Rosemont, là, qui...

Le Président (M. Simard) : Très certainement. Je comprends qu'il y a consentement?

M. Caire : C'est Noël.

Le Président (M. Simard) : M. le député de Rosemont, à vous la parole, pour une période, si je comprends bien, de 4 min 10 s, plus le temps du député de La Pinière. Il lui restait à peu près trois minutes. Donc, voilà, on vous avisera, là, du temps bien précis plus tard.

M. Marissal : Je suis ému. Je suis ému, M. le Président. Merci au collègue de La Pinière. C'est vrai que c'est vraiment intéressant, ce que vous nous dites, M. Sarrazin. Vous avez juste rajouté une couche à des années d'inquiétudes accumulées, là.

Et, en plus, il faut dire que je suis un grand fan, peut-être le fan numéro un, dans cette Assemblée, de la Vérificatrice générale et de ses rapports. D'ailleurs, je vous en pointe deux, que vous avez peut-être lus, sinon vous devriez — puis je n'ai pas beaucoup de questions à vous poser, alors on va profiter de votre présence pour dialoguer un peu — peut-être les partager avec vos étudiants, vos étudiantes.

Le rapport de la Vérificatrice générale de mai 2018, audit de performance sur les reprises informatiques au MTESS — ça, c'est l'aide sociale, notamment, ça, ça fait peur aussi un peu — et un des mes préférés au musée des horreurs, rapport, toujours, de la Vérificatrice générale, juin 2020, *Gestion des identités et des accès informatiques*, et là, tenez-vous bien, à la RAMQ et chez Retraite Québec, qui ne sont pas exactement des dépanneurs, en termes de collecte de données, là, ce serait plutôt des Costco. Ça aussi, ça fait peur un peu.

Mais j'ai quand même une question pour vous. Les huit tests que vous nous avez amenés, là, je pense que c'est assez connu dans votre milieu, là. Je n'aurais pas su les répéter de mémoire, absolument pas, ce n'est pas ma spécialité, mais il n'y a rien non plus qui me renverse là-dedans. De un, est-ce qu'il faut les prendre dans l'ordre que vous avez nommé, c'est-à-dire est-ce qu'il y a une chronologie? Puis, de deux, vous voyez ça où dans un projet de loi comme celui qu'on a devant nous? Autrement dit, comment on légifère ça?

M. Sarrazin (Claude A.) : Ça, c'est une excellente question. Je ne suis pas un juriste, ça fait que je vais avoir beaucoup de difficulté à vous dire comment vous pouvez légiférer ça. Moi, c'est sûr que l'axe de la prévention, pour moi, c'est un essentiel, et je pense que c'est le premier axe, parce que, pour pouvoir évaluer le niveau de protection à mettre en place... je sais que dans le projet de loi, puis, je m'excuse, je ne l'ai pas sous la main, dans le projet de loi, il y avait une évaluation de la menace, là, qui était donnée comme responsabilité. Peut-être qu'on peut le définir d'une autre façon ou augmenter la responsabilité, ça reste entièrement à vous de le voir, mais c'est vraiment de pouvoir évaluer le risque et la menace, parce que, sans ça, on ne sait pas ce qu'on sécurise ou contre qui on le sécurise, ultimement. On sait qu'on a de l'information, on va la protéger. Maintenant, comment qu'on la protège puis à quel niveau qu'on la protège, comment est-ce que ça peut être... cette information-là peut devenir vulnérable et qui peut la vouloir, pour faire quoi?

Il y a tellement de méthodes de fraude, je pourrais vous en parler pendant deux, trois heures, facile, mais, tu sais, la fraude aux prêts hypothécaires, la fraude au point de vue des remboursements au ministère du Revenu... Il y a trois types, l'année dernière ou voilà deux ans, qui ont ramassé 23 millions US en remboursements de l'IRS aux États-Unis, en Albanie. Tu sais, il faut le faire, quand même, là. Ça fait que, donc, bien simplement, la méthode est supersimple, est superconnue, ça fait que, donc, je ne dévoile pas des secrets au grand jour, là, mais c'est ce genre de situations là. Encore une fois, c'est souvent de l'information qui est sous-évaluée au point de vue de la menace qu'elle peut poser.

M. Marissal : Ou alors stockée trop longtemps alors qu'elle n'a plus d'utilité autre que de remonter une chaîne puis d'arriver à quelqu'un.

M. Sarrazin (Claude A.) : Exact.

M. Marissal : ...une gestion d'inventaire, si je peux m'exprimer ainsi, là, ça prend ça aussi. O.K. Je pense que je n'ai plus beaucoup de temps, hein, M. le Président, ça doit être à peu près ça?

Le Président (M. Simard) : 3 min 25 s.

M. Marissal : Qu'il me reste?

Le Président (M. Simard) : Oui, oui, 3 min 25 s. Ah oui, oui!

M. Caire : C'est parce que tu n'es plus habitué, Vincent.

M. Marissal : Non, c'est ça, écoute...

M. Sarrazin (Claude A.) : Juste pour compléter sur ce que je disais, étant donné qu'on a encore du temps, un des exemples où est-ce qu'on néglige la vulnérabilité, c'est souvent l'information sur les enfants. Ce n'est pas encore des payeurs d'impôts, ils ont peu ou pas de compte en banque, bon, ils n'ont pas de revenus, etc. L'information sur les enfants est très recherchée par les fraudeurs pour commettre différents types d'infractions. Ça fait que les cybercriminels vont aller chercher cette information-là, ils vont l'utiliser pour pouvoir commettre différents types de fraudes à partir de ça. Et souvent, c'est une information qu'on considère peu à risque parce qu'on se dit : Ils n'ont pas de risque financier, tu sais. C'est où que ça se passe? Pourquoi que c'est important de protéger de l'information d'un enfant plus que celle d'un adulte, pas nécessairement plus, mais au moins au même niveau?

Ça fait que, donc, il faut la considérer, parce que c'est une information qui va être utilisée. Les crédits d'impôt pour les enfants vont être détournés à partir de l'information concernant l'enfant. Ça fait que, donc, il y a une multitude de méthodes qui peuvent être utilisées.

M. Marissal : Pas super rassurant, considérant ce qu'on a appris, là, il y a deux semaines, sur la liste d'attente, là, du service de garde, 0-5 ans, là. J'oublie le nom exact, mais c'est quelque chose comme ça. Vous en avez vraisemblablement entendu parler, là.

• *(15 h 20)* •

M. Sarrazin (Claude A.) : Oui, mais, dans ce cas-là, là, on parle peut-être d'une action qui était plus ciblée. Je ne connais pas les détails de l'enquête, là, mais de ce que j'ai pu voir, ça semblait être une action plus ciblée, ça fait que... donc, où les gens n'ont pas nécessairement senti le besoin de couvrir leurs traces plus qu'il fallait.

M. Marissal : Juste terminer, M. Sarrazin, avant de vous remercier, vous m'avez fait un peu sourire, tout à l'heure, quand vous avez dit... avec votre exemple d'EncroChat, vous avez dit : Si la police est arrivée à hacker EncroChat,

imaginez, c'est sûr que les cyberpirates peuvent le faire. Moi, il me semble que, dans un monde normal, ce serait le contraire, là, il faudrait plutôt s'étonner que la police ait moins de moyens que les cybercriminels, mais c'est effectivement le monde dans lequel on vit, et puis je le comprends bien.

Je n'ai pas d'autre question. Je sais que vous allez nous envoyer un papier, un document écrit, alors on lira ça avec grand plaisir. Puis je vous invite vraiment à aller lire les deux rapports que je vous ai cités, pointés, de la Vérificatrice générale. Je vous remercie beaucoup.

M. Sarrazin (Claude A.) : Merci.

M. Caire : M. le Président, juste pour dire à M. Sarrazin que, si jamais il a envie d'une job dans la fonction publique, j'ai peut-être quelque chose pour lui.

Le Président (M. Simard) : Bien. Donc, M. Sarrazin, à nouveau, merci pour votre contribution à nos travaux. Ceci met donc fin à notre période de consultations sur le projet de loi n° 95.

Mémoires déposés

Avant de conclure les auditions, je dépose les mémoires des personnes et organismes qui n'ont pas été entendus lors des auditions publiques. À nouveau, merci pour votre précieuse collaboration, en particulier l'équipe du secrétariat, toujours tout aussi efficace, avec un surcroît de difficulté, là, les commissions virtuelles, ça demande un niveau d'agilité technologique décuplé. Donc, merci pour votre patience et votre efficacité.

La commission ajourne ses travaux sine die. Donc, au plaisir de vous revoir.

(Fin de la séance à 15 h 22)