



CFP - 022M  
C. P. - PL 3  
Loi sur les renseignements  
de santé et de services sociaux

PAR COURRIEL

Montréal, le 2 février 2023

Monsieur Jean-François Simard  
Président  
Commission des finances publiques  
Édifice Pamphile-Le May  
1035, rue des Parlementaires, 3<sup>e</sup> étage  
Québec (Québec) G1A 1A3

**Objet : Lettre de recommandations en regard du projet de loi n° 3 *Loi sur les renseignements de santé et de services sociaux et modifiant diverses dispositions législatives***

---

Monsieur le Président,

Depuis 50 ans, Medtech Canada collabore avec les gouvernements, les prestataires et les patients afin de contribuer à l'amélioration de la santé des Canadiens et à la pérennité du système de soins de santé. Au Québec, elle compte plus de 369 entreprises d'équipements, de dispositifs et de services utilisés dans le diagnostic et le traitement des maladies et des problèmes de santé. Le secteur des technologies médicales représente près de 14 000 emplois au Québec.

Medtech Canada met en valeur les nouvelles technologies dans le domaine médical qui sont disponibles sur le marché. L'association est particulièrement intéressée par l'évolution de l'environnement d'affaires qui peut affecter les organisations qu'elle représente pour améliorer la qualité des soins des Québécois.

Medtech Canada est la voix de l'industrie pour tout ce qui concerne l'accès aux technologies médicales, leur intégration dans le système de santé et les enjeux qui affectent l'écosystème du secteur « medtech ».

Nous souhaitons attirer votre attention sur certains éléments du projet de loi n° 3, *Loi sur les renseignements de Santé et de Services sociaux et modifiant diverses dispositions législatives* (PL3) dans le cadre des consultations particulières en cours.

D'entrée de jeu, notre association rappelle que la gestion efficace des données de santé est, dans un système de santé moderne, une nécessité absolue. L'encadrement adéquat de la cueillette, de la transmission et de l'utilisation de ces données que ce soit aux fins de recherche ou pour des raisons cliniques ou administratives, en toute sécurité et dans le respect de la vie privée des

individus est un impératif. C'est d'ailleurs un enjeu mondial. Toutes les juridictions comparables au Québec se dotent de régimes d'encadrement similaires à ce qu'on vise à mettre de l'avant avec le PL3.

Medtech Canada appuie donc avec enthousiasme la modernisation entreprise avec le PL3 pour encadrer plus efficacement la gestion des données de santé au Québec et maintenir un système de santé de classe mondiale qui s'appuie sur celles-ci.

La Commission a l'occasion d'entendre et de prendre connaissance des mémoires présentés par un large éventail de groupes concernés par ce vaste sujet, notamment nos collègues du secteur des sciences de la vie, [BioQuébec](#). Ils illustrent la pertinence d'un encadrement efficace au bénéfice des Québécois, en particulier sur le plan de la recherche, de la qualité, de l'innovation et de la gestion des services de santé. Notre association s'unit à ces représentations et ne ressent pas le besoin de commenter sans ajouter d'éléments nouveaux.

Medtech Canada a plutôt choisi de mettre l'accent sur les articles 84 à 88 du projet de loi qui traitent de la certification de certains produits ou services, dispositions qui touchent plus particulièrement ses membres et qui auront un impact sur l'efficacité du système et sa capacité à accueillir l'innovation.

Le système de santé est soutenu dans son quotidien par l'usage de la technologie médicale, notamment les TI et les applications numériques associées ou non avec les dispositifs et équipements médicaux.

Or, la cybersécurité dans le domaine médical est un enjeu très sensible comme on doit s'y attendre. L'industrie que nous représentons prend ses responsabilités avec rigueur depuis longtemps, et ce, à l'échelle mondiale. Des normes, des protocoles, de meilleures pratiques de l'industrie existent, sont développés par des organismes de réglementation et de certification internationaux dans un souci d'harmonisation mondiale et sont largement utilisés. La plupart des juridictions comparables au Québec appliquent leur cadre normatif propre qui, généralement, reprend des normes généralement reconnues dans l'industrie.

Medtech Canada a d'ailleurs pris [position](#) en ce sens dans le cadre des consultations particulières sur le projet de loi n° 6, *Loi édictant la Loi sur le ministère de la Cybersécurité et du Numérique et modifiant d'autres dispositions* (PL6).

Nous avons la préoccupation que le PL6 puisse avoir un effet sur la « chaîne de commandement » lorsque vient le temps de déterminer les normes et règles applicables pour la sécurité, l'intégration et le développement informatique dans le domaine de la santé.

En effet, bien que le ministère de la Cybersécurité et du Numérique (MCN) soit l'acteur ultime en la matière, le PL3, à l'instar du PL19 qui le précédait, continue selon notre compréhension à entretenir la perception que la responsabilité ultime pouvait être partagée entre deux ministères. Il nous apparaît fort important de limiter le potentiel de conflits ou la tentation de renchérir entre experts interministériels et/ou de supplantation de normes spécifiques à la santé par des normes plus génériques, mais inadaptées.

Fort heureusement, le PL3 attribue clairement la responsabilité au ministre de la Santé et des Services sociaux à l'article 83 de définir par règlement les règles encadrant la gouvernance des renseignements détenus par les organismes.

Nous espérons donc que le ministre de la Santé et des Services sociaux arrimera et coordonnera ses efforts en matière de cybersécurité avec ceux du MCN qui garde, selon la *Loi sur le ministère de la cybersécurité et du numérique* (chapitre M-17.1.1), la mission « d'animer et de coordonner les actions de l'État dans les domaines de la cybersécurité et du numérique, de proposer au gouvernement les grandes orientations en ces domaines, de déterminer les secteurs d'activités où il entend agir en priorité et de proposer au gouvernement des mesures en vue d'accroître l'efficacité de la lutte contre les cyberattaques et les cybermenaces au Québec ».

Nous souhaitons aussi que le PL6 énonce un principe d'harmonisation avec les normes globales généralement reconnues dans l'industrie, de la même manière qu'il fait référence aux « principes de protection des renseignements personnel généralement reconnus » à l'article 38(4<sup>o</sup>), afin de veiller à ce que le Québec ne soit pas géré en isolation en la matière. L'absence d'harmonisation pourrait priver le Québec de solutions de grande valeur et tout à fait sécuritaires.

Nous sommes toujours dans l'attente de réponses en ce sens et espérons que l'étude du présent projet de loi permettra d'y donner suite.

Voici donc nos recommandations concernant le PL3.

### **1) L'article 84 devrait se lire ainsi :**

« Le ministre peut, par règlement, déterminer les mesures de sécurité qui s'appliquent à l'acquisition ou l'utilisation d'un produit ou service technologique.

Il peut également déterminer, par règlement, toute autre exigence d'encadrement eu égard à l'évaluation, la protection des renseignements personnels et la sécurité offerte par le produit ou le service, à ses fonctionnalités et à son interopérabilité avec les autres appareils, systèmes ou actifs informationnels utilisés par les organismes.

L'évaluation de la conformité aux exigences d'encadrement visées par le règlement sont assurées par le ministre ou par toute autre personne ou tout groupement à qui il en confie la responsabilité. »

Un régime de certification seul et local n'atteindra pas, en soi, l'objectif d'assurer la cybersécurité. La cybersécurité est une responsabilité partagée qui s'inscrit sur le cycle de vie du produit ou service, y compris la manière dont sa mise en service et son utilisation sont faites dans le milieu d'accueil. La certification préalable à l'acquisition ou à l'usage n'offre pas les garanties souhaitées. Par exemple, un équipement « certifié », mais non maintenu à jour par l'établissement peut être à risque, sans égard au fait qu'il figure à une liste d'équipements dits certifiés.

Le concept de certification « préalable » est problématique aussi, car l'ampleur du travail requis pour certifier tous les équipements achetés ou utilisés dans le réseau de la santé est

énorme. Par ailleurs, un soumissionnaire dont l'offre serait retenue pourra prévoir de faire les investissements et rehaussements technologiques requis seulement une fois l'assurance reçue que son offre a été acceptée – pour éviter le risque de le faire à perte. Or, la manière dont les devis d'appel d'offres sont conçus dans le réseau de la santé implique que la certification sera une condition de conformité, ce qui serait un frein à l'introduction d'innovations.

Le *Bureau de certification et d'homologation* du Ministère de la Santé et des Services sociaux (qui s'appelle aujourd'hui le *Bureau de certification*) n'a ni la capacité, ni les ressources et ni les moyens pour répondre à ce besoin en temps opportun, quand on considère la nécessité de rehaussement technologique rapide du Québec et en appui du Plan Santé. Une « certification » préalable serait une barrière à l'entrée significative surtout si le processus de certification n'est pas bien adapté à la nature du produit ou au service technologique dont il est question ou si elle implique des frais non négligeables comme c'est le cas aujourd'hui. Elle pourrait limiter les choix offerts dans un contexte d'appel d'offres compétitif en vue d'acquérir des technologies de pointe.

Il faut donc que le pouvoir de régler vise plus large que la certification afin d'éviter le goulot d'étranglement que constituerait une procédure de certification inadaptée alors que d'autres moyens plus efficaces permettent d'atteindre le résultat recherché.

Enfin, il faut éviter qu'un processus de certification propre au Québec émane de l'éventuel règlement alors que des normes internationales généralement reconnues dans l'industrie sont déjà en vigueur et respectées par les fournisseurs et les utilisateurs, et dans le cas des appareils médicaux, font aussi partie de leur évaluation en vue de leur homologation réglementaire dans bien des pays, dont le Canada.

C'est pourquoi nous reprenons ici la recommandation formulée lors de l'étude du PL6, tout comme [l'Association québécoise des technologies](#) (AQT)<sup>1</sup> l'avait fait d'ailleurs, soit la mise sur pied d'un comité avisé en matière de cybersécurité et du numérique afin de conseiller le ministre et de l'appuyer dans la définition des orientations, des programmes, des politiques et des stratégies, et de nous assurer que le domaine des technologies médicales y soit représenté dans l'intérêt des patients.

## **2) L'article 85 est superflu si l'article 84 est modifié, comme suggéré.**

Il est intéressant de noter que l'article 85 tel que rédigé offre une « porte de sortie » aux organismes advenant le cas où la « certification préalable » s'avère irréaliste. Notre proposition permet plutôt de mieux baliser la pratique en permettant au ministre de régler la cybersécurité de manière plus adaptée que par une certification.

## **3) L'article 86 devrait se lire ainsi :**

« Un fournisseur de produit ou service technologique qui, dans le cadre d'un contrat conclu avec un organisme, lui fournit un tel produit ou service visé par l'article 84 est tenu de

---

<sup>1</sup> [https://www.aqt.ca/wp-content/uploads/2021/11/AQT\\_PL6\\_Memoire\\_22nov2021.pdf](https://www.aqt.ca/wp-content/uploads/2021/11/AQT_PL6_Memoire_22nov2021.pdf)

s'assurer que ce dernier respecte les mesures de sécurité et exigences d'encadrement prévues par un règlement pris en vertu de l'article 84 pendant toute la durée de ce contrat.

De même, un organisme qui utilise un produit ou service technologique visé par l'article 84 est tenu de respecter les mêmes mesures de sécurité et exigences d'encadrement. »

Partant du principe que la cybersécurité est une responsabilité partagée entre les fournisseurs, les utilisateurs et les établissements, il nous apparaît nécessaire d'inclure les organismes dans l'article 86. En effet, une fois que le contrat de service qui couvre le produit ou le service technologique est expiré (ou inexistant) les risques de cybersécurité augmentent si l'organisme ne respecte pas les meilleures pratiques et cesse les mises à jour, par exemple. Il faut donc s'assurer de maintenir les mesures de sécurité qui s'imposent.

Nous comprenons par ailleurs que les organismes seront déjà tenus de respecter les règles de gouvernance des renseignements qu'ils détiennent, selon un éventuel règlement adopté en vertu de l'article 83. Il nous semble nécessaire de les assujettir aussi au règlement de l'article 84.

#### **4) L'article 87 devrait être retiré.**

Il nous apparaît inapproprié d'indiquer dans la loi les détails de la certification éventuelle qui feront l'objet d'un règlement prévu à l'article 84. De plus, la portée de l'article tel que présenté soulève des inquiétudes quant à la teneur des renseignements qui pourraient être exigés, notamment des informations commercialement sensibles, confidentielles, touchant la propriété intellectuelle, les codes sources, etc.

Il vaut mieux définir ces exigences dans le cadre de l'élaboration du règlement prévu à l'article 84.

#### **5) L'article 88 devrait être retiré.**

La publication de la liste des produits et services technologiques dits « certifiés » est irréaliste. Une multitude d'équipements sont présentement installés dans le réseau de la santé qui génèrent, transmettent et utilisent des données, ainsi que toutes leurs versions. Le parc d'équipement médical est loin d'être statique, la mise à jour d'une telle liste sera une tâche colossale qui n'apportera pas de valeur.

Nous sommes convaincus que nos recommandations contribueront à faire en sorte que le Québec applique les meilleures pratiques en matière de cybersécurité médicale en s'appuyant sur les normes internationales généralement reconnues. Nous sommes convaincus qu'à l'issue de ces travaux, le Québec sera doté d'un cadre normatif robuste et en phase avec l'industrie, de manière à protéger l'intérêt public et permettre l'accès aux technologies numériques de pointe dans le réseau de la santé.

Nous remercions la Commission de bien vouloir tenir compte de nos recommandations dans le cadre de l'étude du PL3.

Dans le but d'en assurer un suivi approprié, nous souhaitons que cette lettre de recommandation soit déposée à titre de mémoire dans le cadre de l'étude du PL3.

Veillez recevoir, monsieur le Président, mes salutations les plus distinguées.

Le vice-président Québec,



Benoît Larose

- c. c. M. Éric Caire, ministre de la Cybersécurité et du Numérique
- M. Christian Dubé, ministre de la Santé et des Services sociaux
- M. André Fortin, porte-parole de la l'opposition officielle pour la santé
- Mme Michelle Setlakwe, porte-parole de l'opposition officielle pour la protection des renseignements personnels, la cybersécurité et le numérique
- M. Haroun Bouazzi, porte-parole du deuxième groupe d'opposition pour la cybersécurité et le numérique
- M. Vincent Marissal, porte-parole du deuxième groupe d'opposition pour la santé
- M. Joel Arseneault, porte-parole du troisième groupe d'opposition pour la Santé, la cybersécurité et le numérique