TÉLÉTRAVAIL QUÉBEC

CFP - 007M
C.P. - PL 6
Ministère de la Cybersécurité et du Numérique

MÉMOIRE

PRÉSENTÉ À LA COMMISSION DES FINANCES PUBLIQUES

DANS LE CADRE DU PROJET DE LOI N° 6,

Loi édictant la Loi sur le ministère de la Cybersécurité et du Numérique et modifiant d'autres dispositions

24 NOVEMBRE 2021

Introduction

Télétravail Québec est un organisme à but non lucratif ayant notamment pour mission d'améliorer les conditions de travail des Québécois en partageant les meilleures pratiques concernant le télétravail. Les six valeurs de Télétravail Québec sont : l'accessibilité, la sécurité, la conciliation travail-famille, l'équilibre, la saine performance et la protection de l'environnement.

Depuis 2018, et représentant plus de 80 membres, nous encadrons et soutenons des travailleurs et employeurs, partout au Québec. Télétravail Québec représente les intérêts de trois différents profils de membre : les télétravailleurs, les employeurs et les fournisseurs de service.

Les services offerts par l'Association ciblent principalement la diffusion de bonnes pratiques entourant le télétravail et la formation de la main-d'œuvre. En ce sens, Télétravail Québec est l'instigateur de la Semaine du Télétravail, depuis septembre 2020.

Table des matières

Problématiques par rapport à l'indépendance réelle qu'aura le volet Cybersécurité vs Numérique du Ministère

Jean-Philippe Racine, président de la firme Groupe Cyberswat et partenaire de Télétravail Québec, nous explique avoir une préoccupation à ce sujet et souhaite que les impératifs de livraison du volet numérique n'aient pas le dessus sur le volet Cybersécurité. À titre d'exemple, dans une entreprise, il recommande toujours de ne pas mettre le service de cybersécurité sous la direction des technologies de l'information (TI), car il y a un conflit d'intérêts entre la gestion de l'infrastructure TI et la gestion de la cybersécurité. Il est donc primordial que le gouvernement assure une distinction claire entre les TI et la cybersécurité. Qui plus est, il faudrait assurer une séparation étanche entre les deux pour éviter que les intérêts des deux volets s'entremêlent.

Problématiques concernant l'utilisation de réseaux domestiques à des fins commerciales ou d'affaires

La récente directive sanitaire visant à obliger les employeurs à fermer temporairement leurs bureaux et de permettre aux employés de travailler à partir de leur domicile, sans partager de bonnes pratiques à ce moment, à contribuer à une hausse des vols de données et de piratage. L'utilisation des réseaux domestiques à des fins commerciales ou d'affaires est maintenant chose du commun. Cette hausse de l'utilisation de l'Internet résidentiel est un « beau problème » pour certains, mais une opportunité pour les pirates informatiques.

Le gouvernement doit donc clarifier ses intentions en ce qui concerne le télétravail et surtout, comment le tout sera opérationnalisé. Il faut s'assurer que l'utilisation des réseaux domestiques par les fonctionnaires ne viendra pas créer une brèche en matière de cybersécurité.

Problématiques en lien avec l'accès Internet par réseau Wifi public

C'est bien connu, les réseaux Wifi publics sont source de bien des piratages et de vols de données. Pourtant, plusieurs commerces offrent des réseaux Wifi publics, voulant simplement répondre à cette demande de connectivité. Il n'y a aucun moyen pour les clients de savoir si ce réseau est vraiment sécuritaire et actuellement, aucune surveillance ne se fait à ce niveau.

Cependant, le gouvernement devra mettre en place une politique claire en ce qui concerne l'utilisation de réseaux publics par les fonctionnaires. Qui plus est, il faudra voir si chaque ministère est responsable de l'application de cette politique, ou si cette tâche revient au futur ministère de la Cybersécurité et du Numérique. Les deux cas amènent des enjeux distincts en matière de déploiement des infrastructures et surtout, sur qui retombe la responsabilité de gérer ces infrastructures.

Problématiques concernant les appareils informatiques vendus avec des configurations de sécurités minimales ou absentes

Depuis toujours, lors d'un achat d'appareil informatique, la configuration initiale est presque dans tous les cas, la même, un mot de passe absent ou identique pour tous les appareils (admin ou 1234). Cette configuration initiale est responsable de bon nombre de piratages. Elle est même un très bon moyen de piratage parce que les pirates savent bien que, pour la plupart des appareils, une fois les configurations d'origine appliquées, souvent par une simple manipulation, le mot de passe d'origine (admin ou 1234) remplace le mot de passe créé par l'administrateur.

La Californie, en 2020, a justement adopté une loi qui interdit la vente d'appareils avec mot de passe par défaut copieux.

Source : https://leginfo.legislature.ca.gov/faces/billNavClient.xhtml?bill_id=201720180SB327

Il est donc primordial que le gouvernement mette en place des balises claires avec des mesures coercitives adéquates dans le cadre des appels d'offres en TI et cybersécurité. En ce sens, nous invitons le gouvernement à s'inspirer de la Californie pour s'assurer que les fournisseurs soient imputables particulièrement en matière de cybersécurité.

Dans un même ordre d'idées, le gouvernement doit statuer si la gestion des appels d'offres en TI demeure comme elle l'est actuellement, soit à la discrétion des ministères et organismes, ou si celle-ci est rapatriée au sein du futur ministère de la Cybersécurité et du Numérique ou même au Centre d'acquisitions gouvernementales. Dans tous les cas, il faudra s'assurer d'engager le personnel compétent pour s'assurer que les appels d'offres en TI respectent les plus hauts standards de qualité et de sécurité.

Nos recommandations

1. Que les parlementaires reconnaissent la question de conflit d'intérêts et annoncent de quelle façon ils s'assureront que le volet numérique n'aura pas le dessus sur le volet cybersécurité.

2. Que le gouvernement clarifie ses intentions en ce qui concerne l'implantation du télétravail dans la fonction publique et que des mesures soient mises en place pour ne pas délaisser la cybersécurité.

3. Que le gouvernement mette en place une politique claire en ce qui concerne l'utilisation de réseaux publics par les fonctionnaires.

4. Que le gouvernement mette en place des balises claires avec des mesures coercitives adéquates dans le cadre des appels d'offres en TI et cybersécurité, en mettant l'emphase sur la notion d'imputabilité.

5. Que le gouvernement clarifie l'instance qui sera responsable de piloter les appels d'offres en TI et en cybersécurité, afin de savoir si ceux-ci sont rapatriés au sein du futur ministère de la Cybersécurité et du Numérique ou au Centre d'acquisitions gouvernementales.

Pour obtenir des informations supplémentaires

José Lemay-Leclerc
Président de Télétravail Québec
jlemay@teletravailquebec.org
(514) 730-4175

Adresse postale :
505-6300, avenue Auteuil, Brossard (Québec) J4Z 3P2