

Sous réserve de modifications

**Discours de Patricia Kosseim, commissaire à l'information et à la protection de la vie privée de l'Ontario, au forum sur l'information, l'accès et la protection de la vie privée dans les municipalités de l'Association des directeurs généraux, secrétaires et trésoriers municipaux de l'Ontario (ASTMO)
28 mars 2024**

Vers un avenir numérique : concilier innovation et sécurité dans la gouvernance municipale

Introduction

- Bonjour. Merci de m'avoir invitée, je suis ravie d'être de retour parmi vous. Le commissaire adjoint Warren Mar m'accompagne aujourd'hui, et comme le savent bon nombre d'entre vous, il a travaillé dans le secteur municipal et comprend très bien votre réalité.
- Ce secteur regroupe le plus grand nombre d'institutions dont s'occupe notre bureau, et je me réjouis toujours de pouvoir m'entretenir avec vous de questions d'actualité.
- En tant qu'organisme de réglementation, le CIPVP surveille la conformité aux lois ontariennes sur l'accès à l'information et protection de la vie privée, comme vous le savez.
- Mais notre rôle consiste aussi à établir des relations de travail fondées sur la coopération avec les institutions publiques dans l'espoir de réaliser ce que nous souhaitons tous : des communautés solidaires dans lesquelles les Ontariennes et les Ontariens peuvent s'épanouir et prospérer, confiants dans le fait que leurs gouvernements agissent de manière responsable et respectueuse de leurs droits.
- Aujourd'hui, j'aimerais vous parler de la façon de concilier innovation, protection de la vie privée et transparence dans la gouvernance municipale.
- De plus en plus d'institutions publiques se modernisent et innovent en adoptant des technologies modernes, y compris des systèmes d'intelligence artificielle, mais n'oublions pas que pour connaître un succès véritable et durable, les institutions doivent gagner et conserver la confiance du public.

L'innovation et l'IA

- « L'innovation est la capacité à considérer le changement comme une opportunité et non comme une menace », a dit Steve Jobs.
- Une foule de nouvelles technologies promettent d'aider les institutions publiques à améliorer leur efficacité, leur réactivité et leurs services au public.
- Pensons à la gestion des temps d'attente, à la fourniture de services plus rapides et plus personnalisés, aux interventions dans les situations d'urgence et à la prévention des activités criminelles.
- Cependant, notre enthousiasme pour l'innovation doit s'accompagner d'un engagement équivalent en faveur de la reddition de comptes, de la transparence, de la protection de la vie privée et de la sécurité.
- Tous ces éléments peuvent et doivent coexister. Nous pouvons nous réjouir des possibilités que recèle l'innovation pour améliorer notre vie et croire qu'elle donnera de bons résultats, pour autant que nous ayons mis en place des balises et des cadres de gouvernance adéquats.
- Le [Cadre ontarien pour la fiabilité de l'intelligence artificielle](#) en cours d'évolution préconise l'utilisation éthique de l'intelligence artificielle en s'appuyant sur trois priorités :
 1. Aucune activité d'intelligence artificielle secrète
 2. Une utilisation de l'IA en laquelle les Ontariens et Ontariennes peuvent avoir confiance
 3. Une IA qui est au service de tous les Ontariens et Ontariennes
- En 2021, mon bureau a présenté des observations au gouvernement pendant ses consultations sur son projet de cadre. Nous avons recommandé :

- de clarifier les définitions et d'élargir le champ d'application;
 - d'établir des exigences plus strictes en matière de transparence et de reddition de comptes;
 - d'évaluer les risques de manière plus rigoureuse;
 - d'assurer une supervision humaine continue;
 - de prévoir une surveillance forte et indépendante;
 - d'établir un cadre de gouvernance plus complet, qui pourrait prévoir des situations où le recours à l'IA est jugé inapproprié.
- Nous attendons toujours ce cadre de gouvernance complet deux ans plus tard. Mon bureau a publié une [déclaration commune](#) avec la Commission ontarienne des droits de la personne exhortant le gouvernement de l'Ontario à établir un ensemble de règles *contraignantes* plus solides et détaillées concernant l'utilisation des technologies de l'IA dans le secteur public. Nous avons réclamé des balises claires et efficaces qui tiennent compte de la sécurité, de la protection de la vie privée, de la reddition de comptes, de la transparence et des droits de la personne.
 - Nos bureaux se sont engagés à travailler ensemble, et avec le gouvernement, pour que l'IA soit développée et déployée d'une manière éthiquement responsable pour le bien de toute la population ontarienne.
 - Comme vous le savez, l'Ontario n'est pas seul à devoir relever le défi de la gouvernance de l'IA; tout le monde en parle.
 - Et tout le monde parle aussi de l'IA générative.
 - Entre les mains de personnes malveillantes, l'IA générative peut causer des préjudices bien réels, en répandant des informations fausses ou trompeuses qui peuvent ruiner la vie et la réputation des gens, miner la confiance dans les institutions publiques, faire chuter

les cours de la bourse et compromettre gravement les élections et d'autres processus démocratiques.

- En décembre dernier, avec ses homologues fédéral, provinciaux et territoriaux, le CIPVP a publié les [Principes pour des technologies de l'intelligence artificielle \(IA\) générative responsables, dignes de confiance et respectueuses de la vie privée.](#)
- Ces principes visent à atténuer une foule de nouveaux risques liés à l'IA générative, en particulier pour les groupes vulnérables et historiquement marginalisés, et à garantir que tout contenu génératif, y compris le texte, les images, l'audio ou la vidéo, soit clairement identifié comme ayant été créé par l'IA générative.
- En octobre dernier, nous avons également coparrainé [deux résolutions internationales](#) liées à l'IA qui ont été adoptées lors de la 45^e Assemblée mondiale pour la protection de la vie privée.
- L'une de ces résolutions énonce des principes internationaux pour l'élaboration, le fonctionnement et le déploiement de systèmes d'IA générative, renforçant ainsi notre déclaration FPT, et l'autre se concentre plus particulièrement sur l'utilisation de l'IA dans le contexte de l'emploi.
- Dans ce contexte, justement, comme vous le savez peut-être, le gouvernement a adopté le [projet de loi 149](#) dans le cadre de ses réformes visant à œuvrer pour les travailleurs, obligeant les employeurs à indiquer dans leurs annonces publiques de postes s'ils ont recours à l'IA dans le processus de recrutement.
- J'ai comparu devant le comité parlementaire chargé d'examiner ce projet de loi pour affirmer que, si cette mesure est bonne, elle est loin d'être suffisante pour atténuer les risques de l'IA tout au long de la relation de travail et non seulement lors du recrutement, et pour faire face aux risques de l'IA dans tous les secteurs, et pas seulement dans le domaine de l'emploi.
- Notre événement à l'occasion de la Journée de la protection des données, en janvier 2024, avait pour thème l'intelligence artificielle

dans le secteur public. Plus de 2 300 personnes y ont assisté, et la webémission a été regardée au moins 1 300 fois depuis. Ceux qui l'ont manquée trouveront cet excellent débat de notre panel sur notre [chaîne YouTube](#).

- Plus tôt ce mois-ci, mon bureau a publié un [rapport d'enquête concernant la protection de la vie privée](#) qui, pour la première fois, aborde l'utilisation des technologies de l'IA. Nous avons fait enquête sur l'utilisation d'un logiciel de surveillance d'examens recourant à l'IA à l'Université McMaster.
- Pour en savoir plus à ce sujet, vous pouvez lire sur notre site Web mon [billet de blogue](#) intitulé *L'IA sur les campus*.
- Essentiellement, nous avons conclu que d'importantes préoccupations en matière de protection de la vie privée sont soulevées par le recours à cette technologie de l'IA, qui recueille des données biométriques sensibles et surveille les mouvements et le comportement des étudiants pendant les examens à distance pour détecter les cas éventuels de tricherie.
- Notre rapport souligne la nécessité de poser des balises pour encadrer l'adoption et l'utilisation de la technologie de l'IA dans les universités, et formule des recommandations importantes.
- Voici certaines de ces recommandations :
 - consulter les différentes communautés composant le corps étudiant, notamment les groupes vulnérables et historiquement défavorisés qui peuvent être victimes de discrimination ou de préjugés systémiques;
 - donner aux étudiants la possibilité de ne pas subir de surveillance en ligne lors des examens et de choisir plutôt des examens en personne;
 - veiller à ce que les données qui alimentent les algorithmes soient obtenues en conformité avec les lois et règlements pertinents;

- interdire l'utilisation des renseignements personnels des étudiants sans leur consentement pour l'amélioration de produits, la recherche ou l'entraînement des algorithmes.
- Selon un [rapport sur un sondage concernant la cybersécurité](#) que l'Autorité canadienne pour les enregistrements Internet (ou CIRA) a publié récemment, **78 pour 100** des organisations se composant de municipalités, d'universités, d'écoles et d'hôpitaux ont affirmé redouter, avec raison, les cybermenaces découlant de l'IA générative.
- J'exhorte toutes les municipalités qui envisagent d'utiliser l'IA, ou qui l'utilisent déjà, à prendre les mesures nécessaires pour qu'elle respecte la vie privée et les droits des Ontariennes et des Ontariens, et à tenir compte des recommandations des autorités de protection des données du monde entier, y compris celles du CIPVP.
- Je vous invite aussi à prendre part au débat visant à déterminer les balises à poser. Bien que le Cadre ontarien pour la fiabilité de l'intelligence artificielle soit destiné aux institutions du gouvernement provincial, il n'y a aucune raison de principe justifiant que les municipalités, et le secteur public élargi, ne soient pas soumis aux mêmes règles.

Cybersécurité

- J'aimerais maintenant parler de cybersécurité, un problème qui suscite de plus en plus d'inquiétudes dans les institutions publiques ontariennes.
- Les cyberattaques ont fait la manchette récemment; plusieurs ont pris pour cible des municipalités de l'Ontario.
- Je ne peux pas entrer dans les détails, car mon bureau a entamé plusieurs enquêtes. Mais je puis vous dire toutefois que le nombre de cyberattaques que les institutions municipales ont signalées au CIPVP a plus que doublé en 2023 par rapport à l'année précédente.

- Ce phénomène s'est produit dans un contexte où la déclaration des atteintes à la vie privée est volontaire. Il est donc possible que bien d'autres incidents de cybersécurité n'aient pas été déclarés.
- Une chose est sûre : la cybersécurité est devenue un enjeu crucial pour les institutions municipales.
- Lorsque des cyberattaques menacent l'intégrité des services publics, la cybersécurité devient plus qu'une simple question de respect de la loi. Chaque attaque ébranle la confiance du public dans la capacité des administrations à protéger leurs renseignements et à fournir des services essentiels.
- Selon le [sondage de 2023 sur la cybersécurité](#), le secteur des municipalités, des universités, des écoles et des hôpitaux est le plus à risque.
- Ces organisations, y compris les municipalités, représentent une cible particulièrement prisée pour ces attaques en raison des grandes quantités de renseignements personnels dont elles ont la garde et le contrôle.
- Les cybercriminels profitent également du fait que les institutions publiques fournissent des services essentiels dont les résidents dépendent. Ils extorquent de l'argent à ces institutions en les menaçant de paralyser la prestation de services publics essentiels en verrouillant les données, en refusant de les restituer ou en les diffusant sur le Web caché.
- Selon le rapport de CIRA sur un sondage mené auprès de 500 professionnels de la cybersécurité du Canada, plus du tiers (**38 pour 100**) des organisations du secteur des municipalités, des universités, des écoles et des hôpitaux avaient subi une cyberattaque en 2023, et près du quart (**22 pour 100**) avaient été la cible d'une cyberattaque par rançongiciel.
- Parmi ces organisations, **50 pour 100** ont payé la rançon exigée lors de ces attaques.

Contraintes de ressources

- Chaque fois que l'on aborde la question de la cybersécurité dans les municipalités, l'une des principales préoccupations évoquées est le manque de ressources pour s'attaquer à ce problème.
- Selon un rapport d'analyse comparative de la transformation numérique des municipalités canadiennes publié en 2023 ([MNP Digital](#)), **76 pour 100** des municipalités canadiennes ont déclaré que la cybersécurité comptait parmi leurs principales préoccupations. Appelées à indiquer le principal obstacle qui se dressait devant leur organisation, **62 pour 100** ont fait état de ressources insuffisantes.
- Je travaille depuis un certain temps avec le secteur municipal et je sais que de nombreuses petites villes n'ont pas le même niveau d'expertise, d'encadrement et de ressources à consacrer à la cybersécurité que les grandes institutions.
- Une solution possible consisterait à adopter une réponse collective en s'associant à d'autres organisations pour former une sorte de coalition.
- D'après le rapport de CIRA que j'ai mentionné tantôt, **41 pour 100** des organisations du secteur des municipalités, des universités, des écoles et des hôpitaux ont affirmé faire partie d'un groupe ou d'un partenariat visant à rehausser la cybersécurité.
- Le [Modèle opérationnel provincial de cybersécurité de Santé Ontario](#) en est un bon exemple. Il permet à des organismes de soins de santé de toute la province, sans égard à leur taille, de se coordonner et de gérer ensemble des défis en matière de cybersécurité.
- Selon le [Rapport annuel de Santé Ontario sur la protection de la vie privée et la sécurité](#) publié récemment, ce modèle opérationnel a maximisé les économies et les gains d'efficacité des participants grâce au partage des services, et il a permis à de petites entités d'acquérir des cybercapacités.

- Je vous invite à envisager la mise en place d'une coalition semblable et d'une approche coordonnée dans le secteur municipal, si vous n'avez pas encore commencé à le faire.

Feuilles-info du CIPVP sur les rançongiciels et l'hameçonnage

- Pour aider les organisations à lutter contre les cyberrisques, mon bureau a publié diverses ressources, dont nos feuilles-info sur les [rançongiciels](#) et l'[hameçonnage](#), (en anglais seulement).
- Notre feuille-info sur les rançongiciels propose un survol utile des répercussions des rançongiciels sur les organisations et offre de précieux conseils sur la façon de sécuriser votre organisation, notamment :
 - tenir un inventaire qui permet de savoir où et comment l'information circule;
 - classer les éléments du parc informatique en fonction de leur sensibilité et mettre en place des mesures de précaution proportionnelles au niveau de sensibilité des renseignements;
 - mettre en place un programme de gestion des risques qui prévoit des évaluations régulières de la sécurité;
 - veiller à ce que les renseignements personnels et les documents sensibles soient éliminés de façon sécuritaire.
- Ce document propose aussi des recommandations sur la façon de réagir à une cyberattaque et la marche à suivre pour signaler les atteintes à la vie privée à notre bureau et aviser les personnes concernées.
- Si les cyberattaques sont un moyen pour les voleurs de s'emparer d'actifs précieux, l'hameçonnage est l'outil qu'ils utilisent pour pénétrer dans vos systèmes. Notre feuille-info sur le sujet donne des indications précieuses sur la manière de repérer les éventuelles tentatives d'hameçonnage et de vous protéger contre ce type de

piratage psychologique, qui reste l'un des moyens les plus sournois pour les criminels de s'introduire dans votre organisation.

- Les tentatives d'hameçonnage, que ce soit par courriel, message vocal ou texto, ou autre, deviendront de plus en plus insidieuses, car les outils d'IA générative produiront des pièges toujours plus réalistes dans lesquels les employés risqueront de tomber.
- Pour vous protéger contre les attaques d'hameçonnage, vous pouvez :
 - filtrer les messages entrants pour réduire les pourriels et vérifier l'identité des expéditeurs;
 - utiliser des logiciels qui préviennent, détectent et éliminent les logiciels malveillants;
 - tenir à jour les navigateurs et les autres logiciels;
 - limiter les privilèges d'administrateur et l'accès aux renseignements sensibles;
 - chiffrer les documents, appareils et bases de données contenant des renseignements sensibles;
 - donner une formation au personnel afin qu'il reconnaisse les courriels, messages vocaux ou textos suspects et les signale aussitôt à votre service de TI.

L'info, ça compte

- Un épisode récent de notre [balado](#) *L'info, ça compte*, avec Jason Besner du Centre canadien pour la cybersécurité, propose des conseils pratiques aux organisations et aux particuliers pour se protéger contre les menaces numériques.
- J'ai demandé à Jason ce que pouvaient faire les organisations pour lutter à armes égales contre les cybercriminels. Son premier conseil

est de désigner un champion de la cybersécurité au sein de l'organisation.

- Cette personne serait responsable de l'instauration d'une culture de la sécurité, de la sensibilisation et de la formation ainsi que de bonnes pratiques d'hygiène informatique de base.
- La cybersécurité ne concerne pas seulement le service de TI; elle incombe à tous au sein de l'organisation.
- En ce qui concerne la protection des particuliers contre les cybermenaces, il a insisté sur le piratage psychologique faisant partie de l'hameçonnage, qui reste le point de pénétration le plus important et le plus fiable pour les rançongiciels et les cyberattaques.
- Il a donné un conseil simple : être vigilant quand on reçoit une communication. Est-ce que votre directeur municipal, votre directrice des ressources humaines ou votre service de TI vous demande habituellement de virer des fonds, de mettre à jour des renseignements sur les employés ou d'installer une nouvelle application dans votre ordinateur sans contexte approprié?
- Si vous recevez quelque chose qui vous inquiète, n'hésitez pas à poser des questions et à enquêter, et si un message vous semble suspect, signalez-le à votre service de TI et demandez-lui d'y jeter un coup d'œil.

Rapport annuel — Statistiques du CIPVP — Tribunal

- J'aimerais maintenant parler un peu d'accès à l'information.
- Les organisations assujetties à la LAIMPVP doivent présenter leurs statistiques annuelles à notre bureau, notamment le nombre de demandes d'accès reçues et le temps mis à y répondre.
- Merci à tous ceux qui nous ont remis leurs rapports statistiques à temps. Si vous ne l'avez pas encore fait, il vous reste encore quelques jours d'ici la fin du mois pour le faire.

- Nous avons publié dans notre site Web des réponses à des questions fréquentes sur les rapports statistiques, et nous proposons aussi des webinaires qui expliquent le processus de présentation de ces rapports à notre bureau.
- Nous analyserons les rapports reçus pour 2023 et publierons les données dans notre rapport statistique annuel qui paraîtra en juin.
- En attendant, je peux vous donner un aperçu de certains des chiffres provenant de notre propre bureau, qui seront publiés dans notre prochain rapport annuel.
- En 2023, le CIPVP a ouvert **1 121** dossiers en vertu de la LAIMPVP, le nombre le plus élevé dans ce secteur depuis au moins cinq ans. Au total, **868** de ces dossiers portaient sur des appels de décisions rendues dans le secteur municipal à la suite de demandes d'accès à l'information.
- En ce qui concerne le fonctionnement de notre tribunal, j'ai le plaisir d'annoncer que le délai moyen de traitement et de fermeture des dossiers d'appel a diminué de près de **15 pour 100** par rapport à 2022, et de près de **18 pour 100** si l'on tient compte de tous les secteurs, stades et types de dossiers.
- Plus de **85 pour 100** des dossiers ont été réglés par voie de règlement anticipé et de médiation, un taux de réussite que nous sommes parvenus à maintenir pendant trois années consécutives.
- En 2023, notre arriéré était en baisse de **20 pour 100** par rapport à il y a deux ans; du côté de la médiation, l'arriéré a été réduit de moitié par rapport à 2021.
- Notre projet pilote de médiation d'un jour a été couronné de succès, avec un taux de règlement de **90 pour 100** des dossiers simplifiés, qui ont été fermés en 42 jours en moyenne, soit quatre mois de moins que la moyenne générale.

Demandes frivoles et vexatoires et ordonnances marquantes

- Pour gérer les retards et les arriérés, il faut parfois prendre des décisions difficiles. Si le droit d'accès est fondamental, nous devons veiller à ce que chacun puisse exercer ce droit de manière équitable.
- En règle générale, nous traitons les appels selon le principe du premier arrivé, premier servi. Cependant, nous devons parfois imposer des limites au nombre d'appels actifs qu'un auteur de demande peut interjeter à la fois auprès de notre bureau. Nous lui demandons alors d'indiquer les appels qu'il souhaite que nous traitions en priorité et nous mettons les autres en attente. Nous procédons ainsi en dernier recours, surtout quand il y a beaucoup d'appels en attente, afin de garantir une répartition équitable des ressources pour tous les Ontariens et Ontariennes.
- À l'heure actuelle, **5 pour 100** des dossiers actifs sont en suspens en raison de limites relatives au traitement des dossiers.
- Nous imposons de telles limites pour concilier les besoins de tous les utilisateurs de nos services et éviter que le système ne soit surchargé par une seule partie à laquelle il faut affecter une quantité disproportionnée de ressources.
- Pour gérer les ressources limitées dont nous disposons et nous prémunir contre les abus, nous devons également dénoncer les demandes frivoles et vexatoires, tout en veillant à ne pas bafouer les droits fondamentaux des citoyens.
- Une telle décision est très difficile à prendre, mais la loi nous autorise à le faire dans des situations très précises. Pour connaître les facteurs permettant de déterminer si une demande d'accès à l'information est frivole ou vexatoire, je vous invite à consulter notre [bulletin d'interprétation](#) et notre [feuille-info](#) sur ce sujet. Ils sont accessibles sur notre site Web.
- Dans le cadre de sa série « Secret Canada », Tom Cardoso du *Globe and Mail* a écrit au sujet des demandes frivoles et vexatoires, en recommandant aux auteurs de demande de ne pas se montrer

déraisonnables : « Si une institution publique vous a déjà averti qu'elle considère vos demandes comme étant frivoles ou vexatoires, ne prenez pas cet avertissement à la légère. »

Ordonnances marquantes du CIPVP

- J'aimerais maintenant vous faire part de certaines ordonnances portant sur des demandes frivoles et vexatoires qui, je crois, vous intéresseront. Vous trouverez nos ordonnances et décisions dans notre site Web, dans la [section « Décisions »](#).
- **L'ordonnance [MO-4241](#)** portait sur huit appels de deux demandes déposées par l'avocat de plaignants dans une poursuite en recours collectif intentée contre une municipalité. Les demandes concernaient des documents sur le processus de proposition, d'examen et d'approbation d'aménagement du lotissement Saw-Whet.
- La ville d'Oakville a refusé l'accès sous prétexte que les demandes étaient frivoles ou vexatoires.
- Le CIPVP a confirmé cette conclusion de la ville, car l'appelant avait eu une conduite manifestant un abus du droit d'accès à l'information. Il semblait également que le nombre de demandes déposées n'était pas en voie de diminuer.
- Environ 16 pour 100 des demandes reçues par la ville émanaient de cet appelant, ou d'un autre appelant, qui étaient tous deux parties à la même poursuite en recours collectif et semblaient collaborer.
- Au cours de l'année suivante, le CIPVP a limité l'appelant à une demande active, avec un nombre limité de volets, et à un seul appel actif à la fois impliquant la ville.
- **L'ordonnance [MO-4300](#)** portait sur trois appels de trois demandes formulées par un propriétaire d'entreprise de Brantford.
- La ville a affirmé que l'appelant avait déposé 145 demandes d'accès à de la correspondance entre des membres de son personnel. La ville a répondu à un grand nombre de demandes, mais elle a fini par

refuser l'accès au motif que les demandes étaient frivoles ou vexatoires.

- Le CIPVP a constaté que de nombreuses demandes étaient redondantes, excessivement générales et anormalement détaillées. Il semblait que l'appelant essayait d'entraver le système avec ses demandes.
- Le CIPVP a limité l'appelant à une demande d'accès à la ville, avec un nombre limité de volets, et à un appel devant le CIPVP pendant un an.
- **L'ordonnance [MO-4468](#)** portait sur un avocat représentant des plaignants dans un recours collectif qui avait présenté une demande d'accès à plusieurs volets à un office de protection de la nature.
- L'office a affirmé qu'il était surchargé par le nombre de demandes soumises par l'équipe juridique chargée de la poursuite en recours collectif.
- Le CIPVP a conclu que l'appelant avait présenté des demandes répétées ou semblables, et que sa demande d'accès à plusieurs volets reflétait une conduite, car il y avait au total 37 demandes.
- Le CIPVP n'a pas conclu que l'appelant cherchait à entraver le système, mais il reste que ses actes ont donné lieu à un abus du droit d'accès.
- **L'ordonnance [MO-4493](#)** portait sur le canton d'Oro-Medonte. Le canton a reçu une demande à trois volets de la part d'une personne faisant partie d'un groupe qui poursuivait le canton au sujet de certains frais d'utilisation du réseau d'aqueduc et de la propriété de ce réseau.
- Le canton a refusé l'accès au motif que les demandes étaient frivoles ou vexatoires, affirmant que leur auteur avait déposé 35 demandes d'accès, chacune ayant donné lieu à un appel, et portant toutes sur la même question.

- Même si l'appelant avait un réel intérêt pour les renseignements, sa demande a été considérée comme reflétant une conduite visant à surcharger la municipalité alors qu'elle était déjà confrontée à des demandes d'accès et à des litiges connexes.
- L'appel a été rejeté.
- Je ne vous parle pas de ces ordonnances pour que les institutions refusent les demandes d'accès légitimes d'auteurs de demande au motif qu'elles sont frivoles ou vexatoires. Des demandes ennuyeuses, gênantes ou coûteuses en ressources ne sont pas nécessairement frivoles ou vexatoires.
- Je mentionne ces ordonnances récentes pour montrer plutôt que la loi prévoit cette exception pour une raison bien précise, et que le CIPVP confirmera son application dans des situations appropriées, si les conditions sont remplies.

Documents d'orientation du CIPVP

- Avant de terminer, j'aimerais vous parler de notre dernier document d'orientation et d'autres ressources.

Document d'orientation sur les fournisseurs externes

- J'ai le plaisir de vous annoncer la publication prochaine d'un nouveau document d'orientation du CIPVP, *La protection de la vie privée et l'accès à l'information dans les contrats du secteur public avec des fournisseurs externes*.
- Nous sommes encore en train d'y apporter les dernières touches en vue de sa publication dans les semaines à venir. Je remercie l'ASTMO d'avoir formulé des commentaires utiles sur une version antérieure de ce document d'orientation.
- Je vous l'ai déjà dit et je le répète : vous pouvez externaliser des services, mais pas votre obligation de rendre compte.

- Ce document d'orientation apporte une aide précieuse au secteur public de l'Ontario quant aux aspects relatifs à l'accès à l'information et à la protection de la vie privée qui doivent être intégrés dans les accords d'externalisation conclus avec des tiers.
- Vous trouverez des recommandations qui s'appliquent à toutes les étapes du processus d'approvisionnement, y compris la planification, les appels d'offres, les contrats, la gestion des fournisseurs et la résiliation du contrat ou de l'accord.
- Ce document sera accessible sous peu dans notre [site Web](#) et je vous invite à le consulter et à en faire part à vos réseaux.

Mise à jour du Code de procédure pour les appels interjetés en vertu de la LAIPVP ou de la LAIMPVP

- Mon bureau travaille également à la mise à jour du [code de procédure](#) pour les appels interjetés en vertu de la LAIPVP ou de la LAIMPVP. La dernière révision remonte à 2004.
- Nous croyons que cette révision est nécessaire pour :
 - refléter les procédures actuelles du CIPVP quant au traitement des appels, y compris les appels déposés par voie électronique;
 - permettre le traitement plus rapide des appels;
 - faire en sorte que l'examen des appels demeure juste et équitable;
 - décrire avec plus de transparence et de clarté les procédures que suit le CIPVP relativement aux appels.
- Nous avons tenu des consultations lors desquelles nous avons invité des institutions publiques et d'autres parties intéressées à nous faire part de leurs commentaires. Nous en avons reçu beaucoup et nous vous en remercions. Nous en tenons compte actuellement pendant que nous finalisons le code de procédure mis à jour.

- Le code de procédure révisé sera publié bientôt dans notre site Web.

Bulletins d'interprétation

- Une autre chose que vous trouverez vraiment utile à mon avis est une nouvelle série de [bulletins d'interprétation](#) que nous avons élaborée afin de décrire comment le CIPVP et les tribunaux interprètent certaines dispositions de la LAIPVP et de la LAIMPVP dans le cadre des appels.
- Ces bulletins d'interprétation peuvent aider les organisations à prendre des décisions mieux éclairées dès le stade de la demande, et ils indiquent aux parties aux appels interjetés auprès de notre bureau à quoi elles peuvent s'attendre et comment elles peuvent améliorer la qualité de leurs observations.
- Les sujets traités actuellement sont les suivants :
 - Garde ou contrôle
 - Les droits et leur suppression
 - Renseignements personnels
 - Recherche de documents pertinents
 - Demandes frivoles et vexatoires
- Nous publions régulièrement de nouveaux bulletins; les tout derniers traitent des sujets suivants :
 - Conseils ou recommandations
 - Nécessité manifeste de divulguer les renseignements dans l'intérêt public
 - Renseignements de tiers
 - Intérêts économiques
- N'hésitez pas à nous poser toute question sur nos bulletins ou à nous suggérer d'autres sujets.

Défi de la transparence

- Une dernière chose avant de terminer : le CIPVP a lancé son deuxième [Défi de la transparence](#)!
- J'ai accordé dernièrement une [entrevue](#) à la revue *Municipal World* au sujet de cette initiative, et j'ai précisé que le Défi de la transparence fait partie des mesures que prend mon bureau pour bâtir une culture de la transparence dans les institutions publiques.
- La transparence et l'accès à l'information sont essentiels dans notre démocratie. Ils permettent de demander des comptes aux pouvoirs publics, de lutter contre la désinformation, de favoriser l'engagement civique et de susciter la confiance du public.
- Cette année, dans le cadre du Défi de la transparence, nous invitons encore une fois les institutions publiques à partager leurs approches novatrices dans le domaine des données ouvertes et de la transparence du gouvernement.
- Nous avons ajouté une nouveauté cette année : nous demandons aux institutions de nous faire part de leurs initiatives uniques de transparence dans la collecte, l'utilisation ou la divulgation de données personnelles.
- Nous espérons faire ressortir l'esprit de compétition des institutions publiques pour qu'elles relèvent le défi de cette année!
- Certains des projets soumis cette année seront mis en vedette dans une nouvelle galerie de notre [Vitrine de la transparence](#) qui sera dévoilée en septembre 2024.
- Pour vous donner un aperçu de ce qui se trouve actuellement dans notre exposition, j'aimerais partager avec vous quelques-uns des excellents projets que des municipalités nous ont soumis l'année dernière.

Ville de Barrie

- L'[initiative](#) de la ville de Barrie consiste en une application mobile qui donne aux résidents l'accès à des renseignements sur les services municipaux populaires.
- Grâce à cette application, les résidents peuvent obtenir rapidement et facilement des renseignements sur les événements, les travaux de voirie, les élections municipales, les réunions du conseil municipal, les transports en commun et le stationnement, des avis publics, les demandes d'accès à l'information, et bien plus.
- J'aime bien aussi que cette application puisse être personnalisée et permette de s'abonner ou de se désabonner à des avis.

Ville de Brampton

- La ville de Brampton publie en ligne des renseignements sur les [demandes d'accès](#) reçues, montrant les documents qui ont été divulgués en vertu des lois sur l'accès à l'information.
- Lorsqu'elle reçoit une demande d'accès à l'information, la ville crée un index comprenant un résumé de la demande, une liste des documents pertinents avec les numéros de page, des précisions sur les dispositions applicables de la loi, le type d'accès accordé et des commentaires.
- La ville publie ces index en ligne, avec des renseignements sur sa réponse à chaque demande d'accès à l'information qu'elle reçoit en vertu de la LAIMPVP.
- Le public peut ainsi avoir une bonne idée des demandes d'accès à l'information que la ville reçoit et de la façon dont elles sont traitées.

Ville de Whitby

- La ville de Whitby a créé un [outil en ligne](#) pour l'élection municipale de 2022 afin de permettre aux candidats de partager leur programme

et aux électeurs d'accéder beaucoup plus facilement à des renseignements pour les aider à faire leur choix.

- Voilà un excellent exemple de la façon dont les données ouvertes peuvent avoir des retombées positives directes sur l'engagement civique.
- Ce nouvel outil permet aussi aux électeurs de confirmer facilement qu'ils figurent sur la liste électorale et de vérifier l'emplacement des bureaux de scrutin.
- D'après un sondage, 96 pour 100 des électeurs étaient satisfaits de cet outil, et 70 pour 100 ont affirmé que sa fonction la plus utile était celle qui leur permettait d'accéder à des renseignements sur les candidats.

Ville de Guelph

- Le [GeoDataHub](#) de la ville de Guelph utilise la technologie des systèmes d'information géographique pour afficher des informations utiles sur ce qui se passe dans la ville.
- Il procure un accès en ligne facile aux ensembles de données ouvertes de la ville sur l'emplacement des chasse-neige, des parcs, des arrêts d'autobus, des parcs de stationnement, et plus encore.
- Les résidents peuvent aussi ajouter des renseignements sur ces événements et des activités qui ont lieu dans leur localité.
- Il s'agit d'une excellente ressource qui favorise l'engagement communautaire et permet aux résidents de combiner des ensembles de données et d'effectuer leurs propres analyses personnalisées à l'aide de cartes et de graphiques.
- J'espère que vous prendrez plaisir à découvrir ces exemples et d'autres dans notre galerie virtuelle et que cela vous donnera envie de soumettre votre propre projet cette année. C'est une excellente occasion pour votre organisation de démontrer son engagement en faveur du gouvernement ouvert et de la transparence.

- La date limite est le **31 mai 2024**, alors il vous reste beaucoup de temps pour nous soumettre votre projet.

Conclusion

- Pour conclure, je tiens à dire que le commissaire adjoint Warren Mar et moi accordons une grande importance aux relations entre le CIPVP et le secteur municipal, qui reposent sur la communication, la collaboration et la coopération.
- Nous aspirons à être un organisme de réglementation moderne et efficace dont les activités ont des retombées tangibles. Pour réaliser cette vision, nous devons entendre et comprendre le point de vue de ceux d'entre vous qui sont en première ligne, qui servent les Ontariennes et les Ontariens au niveau local et communautaire, et qui observent directement ces retombées tangibles sur leurs droits en matière de protection de la vie privée et d'accès à l'information.
- J'ai été encouragée de lire dans les [observations de l'ASTMO](#) sur la modernisation de la *Loi sur l'accès à l'information municipale et la protection de la vie privée* que « les municipalités considèrent la transparence comme un outil important pour susciter et conserver la confiance du public et reconnaître l'importance de l'amélioration continue ».
- Sur ce point, nous sommes tout à fait d'accord.
- Ainsi, dans un esprit de collaboration mutuelle et d'apprentissage continu, Warren et moi nous ferons un plaisir de répondre à vos questions et commentaires.
- Merci.