Sous réserve de modifications

Allocution de Patricia Kosseim, commissaire à l'information et à la protection de la vie privée de l'Ontario
Conférence de la section canadienne de l'Institut international des communications
22 octobre 2024

Le CIPVP : planifier l'avenir numérique des Ontariennes et des Ontariens

Introduction

- Bonjour à tous.

- C'est un plaisir d'être parmi vous aujourd'hui, et je tiens à remercier l'Institut international des communications de cette occasion de vous parler d'une chose qui concerne chacun d'entre nous : notre avenir numérique.

- En 1921, Christian Lous Lange, lauréat du prix Nobel de la paix, en abordant l'essor rapide des technologies industrielles et le risque qu'à moins d'être encadrées, elles dominent la société, a déclaré que « la technologie est un serviteur utile mais un maître dangereux ».

- Un siècle plus tard, ces mots sont plus pertinents que jamais.

- En fait, selon un lauréat plus récent du prix Nobel, Geoffrey Hinton, « nous nous approchons du moment où les ordinateurs pourront se perfectionner d'une manière qui échappe à notre contrôle, ce qui pourrait signifier la fin de l'humanité ».

- La technologie redessine rapidement le monde et on est en droit de se demander si nous en sommes toujours les maîtres, ou désormais les serviteurs.

- Avec en toile de fond ce grand débat existentiel sur l'avenir de l'humanité, nous nous efforçons, ici et maintenant, de déterminer les avantages et les préjudices possibles des technologies émergentes.

- Pendant que les organisations se modernisent et que les nouvelles technologies transforment le monde qui nous entoure en nous

rendant la vie plus facile et plus intelligente, et en nous rapprochant les uns des autres, nous ne devons pas perdre de vue le facteur le plus crucial pour le succès de cette transformation : la confiance du public.

- Je crois que la confiance du public est la base sur laquelle nous devons nous appuyer et en regard de laquelle nous devons mesurer nos efforts.

- Sans elle, l'innovation ne donnera pas lieu à des progrès technologiques dont toute l'humanité pourra profiter. Elle créera plutôt un monde où l'incertitude règne et où les disparités se creusent, ce qui risque d'être dangereux, voire destructeur.

- Pour gagner la confiance du public, les organisations doivent adopter un comportement responsable qui recevra l'aval de la société sur le plan moral et éthique. Pour ce faire, elles doivent faire preuve d'une transparence irréprochable et d'une responsabilité manifeste, et communiquer de façon pertinente avec le public.

- Parfois, cette communication peut avoir lieu directement entre les organisations et leurs clients, ou entre les gouvernements et les citoyens.

- Mais plus souvent, dans un environnement complexe caractérisé par des risques élevés et une forte incertitude, la confiance du public repose sur un intermédiaire : un organisme de réglementation indépendant.

- Un tel organisme peut démêler toute cette complexité, ses tenants et ses aboutissants, et rassurer le public en veillant à ce que tout soit conforme.

- C'est là un défi de taille dans la nouvelle ère où nous vivons, et où les progrès rapides des communications numériques et de l'intelligence artificielle se font sentir dans tous les aspects de notre quotidien.

- Dans la conjoncture actuelle, être un organisme de réglementation efficace nécessite une démarche différente de celle que nous aurions adoptée il y a dix ans.

- L'époque où l'on vérifiait la conformité en fonction de critères fixes, où on enquêtait sur des plaintes au cas par cas après coup et où on assurait le respect de lois statiques est bien révolue, car elle ne correspond plus à la réalité d'aujourd'hui.

- En tant qu'organisme de réglementation, il est de plus en plus difficile de se prononcer sur ce qui est conforme et sur ce qui ne l'est pas, dans un contexte où les lois en vigueur ont été adoptées à une époque où on ne pouvait même pas imaginer les technologies que nous cherchons à régir.

La vision du CIPVP : un organisme de réglementation moderne et efficace ayant une influence concrète

- C'est pourquoi, il y a quatre ans, lorsque j'ai entamé mon mandat de commissaire à l'information et à la protection de la vie privée de l'Ontario, j'avais pour ambition de faire du CIPVP un organisme de réglementation moderne et efficace ayant une influence concrète.

- Une organisation tournée vers l'avenir et se fondant sur des pratiques réglementaires modernes et souples qui encouragent un comportement responsable et favorisent un avenir numérique inclusif, où chacun est protégé et dont les avantages sont à la portée de tous.

- C'est envisager les choses de l'extérieur plutôt que de l'intérieur.

- En d'autres mots, il faut déterminer l'impact que nous voulons avoir dans la réalité, puis agir de façon pertinente pour que cet impact se concrétise, au lieu de nous appuyer sur des mécanismes et processus internes en espérant que l'effet souhaité finira par se matérialiser.

- En établissant des rapports fondés sur la collaboration et la consultation avec d'autres organisations qui travaillent sur le terrain, nous cherchons à créer une culture où le respect de l'esprit, sinon de

la lettre, de la loi fait partie de ce résultat souhaitable au lieu d'être un palliatif.

- Notre bureau a pour vision de renforcer la confiance des Ontariennes et des Ontariens dans le respect de leurs droits en matière d'accès à l'information et de protection de la vie privée par les moyens suivants :

    - la **promotion**, en défendant activement leurs droits dans les domaines stratégiques clés qui ont une incidence sur leur vie;

    - la **pertinence**, en traitant les plaintes et les appels de façon équitable et pertinente, en temps opportun;

    - la **responsabilité**, en maintenant la confiance des Ontariennes et des Ontariens dans l'excellence organisationnelle de notre bureau et dans notre efficacité en tant qu'organisme de réglementation.

- Voilà de bien belles paroles, mais qu'est-ce que tout ça veut dire concrètement?

- Laissez-moi vous donner quelques exemples.

Exemples de ce que fait un organisme de réglementation moderne et efficace ayant une influence concrète

- Lorsque l'article 61.1 de la LPRPS et une disposition connexe d'un règlement d'application [art. 35 de l'Règl. de l'Ont. 329/04] sont entrés en vigueur le 1er janvier 2024, nous conférant le pouvoir d'imposer des pénalités administratives pécuniaires (PAP), nous avons exposé d'emblée notre position à ce sujet.

- Les PAP pourraient se révéler pertinentes dans les cas les plus graves, mais nous continuerons de privilégier l'information, l'orientation et les conseils en montrant de façon proactive aux institutions quoi faire pour respecter les lois ontariennes sur l'accès à l'information et la protection de la vie privée.

- Nous continuerons à miser sur le règlement anticipé et la médiation, en indiquant aux organisations comment rectifier leurs erreurs ou omissions et donner suite rapidement aux leçons apprises, au lieu de nous contenter d'attendre qu'elles commettent de nouvelles erreurs et de leur infliger une amende après coup.

- Autre exemple : nous avons fait un pas en avant en mettant à jour notre *Manuel d'examen et d'approbation des personnes et entités prescrites* en vertu de la *Loi de 2004 sur la protection des renseignements personnels sur la santé*, la LPRPS.

- Nous avons modernisé ce manuel en tenant compte des nouveaux risques pour la sécurité et des nouvelles cybermenaces avec lesquels les institutions sont confrontées pour s'assurer non seulement qu'elles respectent la loi, mais également qu'elles font preuve de résilience dans le monde changeant d'aujourd'hui.

- Ce manuel adopte une approche fondée dans une plus grande mesure sur les risques, et traite de façon plus précise et approfondie d'aspects clés présentant un risque élevé, au lieu d'envisager la conformité de façon superficielle, en cochant des cases sur une liste.

- Pour mieux répondre aux plaintes de façon pertinente et en temps opportun, nous avons apporté des changements importants à notre code de procédure pour les appels interjetés en vertu de la *Loi sur l'accès à l'information et la protection de la vie privée* (LAIPVP) et de la *Loi sur l'accès à l'information municipale et la protection de la vie privée* (LAIMPVP). Ces changements sont entrés en vigueur le **9 septembre**.

- Nous avons notamment instauré un processus d'appel accéléré pour faciliter le règlement des affaires simples, ce qui permet de réduire considérablement les délais de traitement.

- D'autres changements portent sur le resserrement des échéanciers, des limites quant au nombre de dossiers traités et la fermeture de dossiers abandonnés.

- Ces changements s'inscrivent dans notre engagement d'être plus pragmatiques et pertinents, d'assurer le traitement plus rapide des appels et de donner aux parties les réponses dont elles ont besoin pour pouvoir tourner la page et prendre des décisions éclairées.

- Il s'agit donc d'améliorer notre efficacité, de traiter équitablement tous ceux qui font appel à nos services, d'être comptables à la population ontarienne et d'optimiser l'utilisation des ressources limitées dont nous disposons dans un monde de plus en plus axé sur les données, tout en respectant les règles d'équité procédurale et en faisant preuve de transparence quant à nos procédures d'appel.

- Dans une décision rendue il y a quelques semaines, la Cour supérieure de justice a réitéré le principe de longue date voulant qu'elle n'intervienne pas dans les instances administratives, sauf dans des circonstances exceptionnelles.

- La cour a reconnu que le CIPVP, comme tous les tribunaux administratifs, dispose de ressources limitées et devrait jouir de la latitude nécessaire pour établir des pratiques administratives générales et des procédures.

- Au début de l'année, en février, nous avons lancé aux institutions publiques ontariennes notre deuxième Défi de la transparence, en les invitant à faire part de leurs projets créatifs visant à favoriser les données ouvertes et la transparence.

- Notre galerie virtuelle 3D met en vedette bon nombre de ces projets novateurs qui favorisent la transparence du gouvernement et montrent à la population ontarienne les avantages des données ouvertes.

- Nous voulons donner des exemples positifs de projets d'institutions publiques ontariennes et encourager d'autres institutions à faire preuve de plus de transparence.

- C'est un moyen pour nous, en tant qu'organisme de réglementation, de souligner le bon travail des institutions publiques, et pas seulement leurs lacunes.

- Une partie de notre mandat consiste à présenter des commentaires concernant l'incidence sur l'accès à l'information et la protection de la vie privée des projets législatifs ou des programmes gouvernementaux proposés et des pratiques existantes ou proposées relatives aux renseignements des dépositaires de données.

- Nous invitons les organisations à faire appel à mon bureau pour des consultations sur les politiques et pour obtenir nos commentaires sur les conséquences pour la protection de la vie privée et la transparence de nouveaux programmes, projets ou procédés ou de nouvelles technologies.

- Pour structurer ce processus, nous avons établi il y a environ deux ans des lignes directrices sur les consultations afin de préciser les attentes, de clarifier la portée des engagements de confidentialité et d'assurer l'impartialité.

- Nous espérons faire de ce processus de consultation sur les politiques un genre de bac à sable réglementaire, et nous envisageons cette possibilité actuellement.

- Cela m'amène à notre balado *L'info, ça compte*, qui propose des entretiens de fond avec des gens de tous les horizons sur un large éventail de sujets ayant trait à l'accès à l'information et à la protection de la vie privée.

- Nous rencontrons les gens là où ils se trouvent, et nous rendons nos entretiens accessibles à un large public, sous une forme différente.

- Et en tant qu'organisme de réglementation, nous devons avoir l'humilité de poser des questions, être ouverts à différents points de vue, écouter et apprendre comme tout le monde, sur le même pied.

Priorités stratégiques

- Pour être moderne et efficace, un organisme de réglementation doit également se concentrer sur des priorités stratégiques, au lieu d'essayer de s'occuper de tout et de s'éparpiller.

- Le travail du CIPVP est orienté par quatre priorités stratégiques.

- Pour élaborer ces priorités et les objectifs connexes, nous avons recueilli des commentaires des parties prenantes, des institutions que nous supervisons et du public que nous servons, en nous concentrant sur les domaines où nous sommes le plus susceptibles d'avoir le plus d'impact positif pour les Ontariennes et les Ontariens.

- Ces priorités sont les suivantes.

- ***La protection de la vie privée et la transparence dans un gouvernement moderne.*** Notre objectif concernant cette priorité consiste à faire valoir les droits des Ontariennes et des Ontariens en matière de protection de la vie privée et d'accès à l'information en collaborant avec les institutions publiques pour établir des principes fondamentaux et des cadres de gouvernance exhaustifs en vue du déploiement responsable de technologies numériques, y compris l'IA.

- Dans le cadre de notre priorité ***Les enfants et les jeunes dans un monde numérique***, nous défendons les droits des enfants et des jeunes en matière de protection de la vie privée et d'accès à l'information en favorisant leur littératie numérique et l'expansion de leurs droits numériques, tout en tenant les institutions responsables de protéger les enfants et les jeunes qu'elles servent.

- Pour notre priorité ***La nouvelle génération des forces de l'ordre***, nous contribuons à renforcer la confiance du public dans les forces de l'ordre en travaillant avec les partenaires concernés pour élaborer les balises nécessaires à l'adoption de nouvelles technologies et d'approches communautaires qui protègent à la fois la sécurité publique et les droits des Ontariennes et Ontariens en matière d'accès à l'information et de protection de la vie privée.

- Et pour notre priorité ***La confiance dans la santé numérique***, nous favorisons d'une part la confiance dans le système de soins de santé numérique en nous assurant que les dépositaires de renseignements sur la santé respectent les droits de la population ontarienne en matière de protection de la vie privée et d'accès à l'information, et d'autre part l'utilisation novatrice des renseignements personnels sur la santé à des fins de recherche et d'analytique dans la mesure où elle sert le bien public.

- Comme vous pouvez le constater, ces quatre priorités stratégiques consistent à obtenir des avantages importants pour la société, que ce soit sur le plan des services gouvernementaux, de l'éducation publique, de la santé ou de la sécurité publique, en collaborant avec d'autres parties prenantes pour établir de façon proactive des balises et des cadres de gouvernance qui permettent aux institutions de déployer des technologies de façon responsable, transparente et comptable au public, dans le respect des droits fondamentaux en matière d'accès à l'information et de protection de la vie privée.

- Un thème commun de ces quatre priorités stratégiques réside dans la nécessité d'une réforme et d'une modernisation législatives.

- En mai dernier, le gouvernement a réagi en déposant le projet de loi 194, la *Loi de 2024 visant à renforcer la cybersécurité et la confiance dans le secteur public*.

- L'annexe 1 établit des exigences concernant la cybersécurité et l'IA pour les entités du secteur public, ainsi que des règles sur l'utilisation des technologies numériques touchant les enfants et les jeunes de moins de 18 ans.

- L'annexe 2 modifie la *Loi sur l'accès à l'information et la protection de la vie privée* en instaurant des mesures plus solides de protection de la vie privée et en renforçant la surveillance.

- Bien que ce projet de loi aborde directement des questions d'actualité et représente une première étape prometteuse, des améliorations s'imposent de toute évidence.

- Mon bureau a présenté ses recommandations à l'Assemblée législative en vue de renforcer encore plus ce projet de loi.

- Vous pouvez consulter notre mémoire dans notre site Web, à ipc.on.ca/fr.

- L'un des principaux aspects de ce projet de loi réside dans la création d'un régime de gouvernance de la cybersécurité.

- Il est triste de constater la fréquence des cyberattaques dont on parle dans les médias, et de plus en plus d'institutions du secteur public en sont la cible, notamment d'attaques par rançongiciel.

- La ville de Hamilton a subi une telle attaque qui a désactivé presque toutes ses lignes téléphoniques, paralysé le conseil municipal et touché des dizaines de services.

- La ville a dépensé des millions de dollars pour rétablir ses systèmes, et elle compte dépenser près de 34 millions de dollars de plus de 2025 à 2033 pour renforcer sa posture en matière de cybersécurité.

- Le printemps dernier, une attaque par rançongiciel contre cinq hôpitaux du Sud-Ouest de l'Ontario a mis leurs systèmes hors service pendant des semaines et a forcé le report de chirurgies et de rendez-vous.

- D'après un reportage, le rétablissement et la mise à niveau des systèmes ont coûté environ 7,5 millions de dollars à ces hôpitaux.

- Le Sondage 2024 sur la cybersécurité de l'Autorité canadienne pour les enregistrements Internet a révélé des statistiques frappantes sur les municipalités, les universités, les écoles et les hôpitaux, qui forment le secteur MUEH.

- Ce rapport, sur un sondage mené auprès de 500 décideurs en cybersécurité du pays, a permis de constater que plus de la moitié (**55 %**) des organisations du secteur MUEH avaient subi une cyberattaque en 2024, par rapport à **38 %** en 2023.

- De ces attaques contre des organisations du secteur MUEH en 2024, **29 %** ont été efficaces, par rapport à **22 %** en 2023.

- Les cybercriminels savent que les institutions publiques traitent de grandes quantités de renseignements personnels, et qu'en cas de cyberattaque, elles ne peuvent pas simplement interrompre leurs activités.

- Elles doivent poursuivre leurs activités et fournir des services essentiels, ce qui les rend particulièrement vulnérables aux attaques par rançongiciel.

- Bien que je sois favorable à l'intention du gouvernement, dans l'annexe 1, de mettre sur pied un régime de gouvernance de la cybersécurité, il faut faire plus pour protéger la vie privée et la sécurité de la population ontarienne.

- Parmi mes recommandations sur la cybersécurité :

    - j'estime que les éléments de base d'un programme de cybersécurité devraient figurer explicitement dans la loi, et que tout règlement régissant un tel programme devrait exiger que ce dernier comprenne de tels éléments;

    - ces éléments de base devraient comprendre l'identification et la gestion des risques de cybersécurité, et des procédures pour minimiser l'impact des incidents de cybersécurité qui surviennent.

- J'ai recommandé également de signaler au CIPVP les incidents de cybersécurité faisant intervenir des renseignements personnels, dans le cadre de l'exigence de signaler les cyberincidents au ministre des Services au public et aux entreprises et de l'Approvisionnement.

- L'annexe 1 du projet de loi cherche également à réglementer l'utilisation de l'IA par les entités du secteur public en prévoyant des dispositions sur la transparence, la reddition de comptes, la gestion des risques, les normes techniques et la surveillance, de même que certaines utilisations interdites en vertu d'un règlement futur.

- Nous recommandons avant tout que la loi encadre clairement l'utilisation des technologies de l'IA, sans laisser ces questions fondamentales être définies plus tard par règlement.

- Dans notre mémoire, nous avons inclus un ensemble de principes que devraient suivre les organisations du secteur public qui élaborent ou déploient des systèmes d'IA; ainsi :

    - Avant d'être adoptées par des entités du secteur public, les technologies de l'IA devraient répondre à des normes indépendantes afin qu'elles soient ***valides et fiables*** et fonctionnent comme prévu.

    - Les systèmes d'IA devraient être ***sécuritaires*** et conçus pour être favorables à la santé physique et mentale des gens, à la sécurité économique et à l'environnement, et ils devraient être surveillés tout au long de leur durée de vie.

    - Les technologies de l'IA devraient assurer la ***protection de la vie privée*** et être élaborées selon une approche fondée sur la protection intégrée de la vie privée, qui prévoit et atténue les risques pour la vie privée des particuliers et des groupes.

    - Des politiques et pratiques ***transparentes*** devraient être adoptées afin d'informer les gens lorsqu'ils interagissent avec l'IA d'expliquer quand et comment des décisions ont été prises à leur sujet au moyen de l'IA.

    - Une structure de gouvernance ***responsable*** doit être mise en place pour que les particuliers puissent contester l'exactitude des décisions prises à leur sujet et obtenir réparation.

    - Surtout, les technologies de l'IA devraient ***affirmer les droits de la personne*** en étant justes et équitables pour tous les particuliers et toutes les communautés.

- Ce dernier point revêt une importance particulière compte tenu de la discrimination et des préjugés historiques dont font l'objet des communautés marginalisées. Il serait donc judicieux de consulter ces communautés aux fins de l'élaboration et du déploiement de

systèmes d'IA et des règles auxquelles ces systèmes seraient assujettis.

- Mon autre recommandation clé réside dans la nécessité d'assurer une surveillance et une application indépendantes. Les organisations du secteur public devraient être soumises à l'examen d'un organisme de surveillance indépendant habilité à faire respecter ces principes. Sinon, le gouvernement se surveille lui-même, ce qui n'est guère utile.

- Ces recommandations vont dans le sens de la déclaration commune que nous avons publiée l'an dernier avec la Commission ontarienne des droits de la personne exhortant le gouvernement provincial à élaborer et à poser des balises efficaces pour l'utilisation des technologies de l'IA dans le secteur public, en tenant compte de la sécurité, de la protection de la vie privée, de la responsabilisation, de la transparence et des droits de la personne.

- Elles concordent également avec les principes que nous avons établis de concert avec nos homologues fédéral, provinciaux et territoriaux pour des technologies d'IA générative responsables, dignes de confiance et respectueuses de la vie privée; ces recommandations reprennent plusieurs de ces principes visant à réduire les risques pour la vie privée et à promouvoir le développement sécuritaire de technologies d'IA.

- Et elles vont également dans le sens de deux résolutions adoptées à l'unanimité à la 45e Assemblée mondiale pour la protection de la vie privée, qui réunit plus de 130 autorités de la protection des données du monde entier. Ces résolutions portaient sur les systèmes d'intelligence artificielle générative et l'autre sur l'intelligence artificielle et l'emploi.

- L'annexe 1 propose également de réglementer, par des directives ministérielles et des règlements, les technologies numériques destinées aux enfants et aux jeunes de moins de 18 ans.

- Nous avons souligné la nécessité de créer et d'appliquer des normes relatives aux technologies numériques qui respectent les droits des

enfants et des jeunes et qui sont conformes aux valeurs que sont l'autonomie personnelle, la dignité et l'autodétermination.

- Nous avons également recommandé de retirer du projet de loi certaines dispositions qui prescrivent comment les conseils scolaires et sociétés d'aide à l'enfance peuvent recueillir, utiliser, conserver et divulguer des renseignements numériques, car elles risquent de faire double emploi avec les lois existantes sur la protection de la vie privée et donner lieu à des exigences incohérentes.

- Nous recommandons plutôt de renforcer les mesures de protection de la vie privée des enfants et des jeunes des lois actuelles sur la protection de la vie privée, dans le cadre d'un régime réglementaire de protection de la vie privée plus cohérent et homogène.

- Concrètement, il s'agirait de considérer les renseignements personnels des enfants comme étant des renseignements de nature délicate, dont il faut tenir compte dans le cadre d'évaluations de l'impact sur la vie privée, par exemple, ou en vue de prendre des mesures de précaution raisonnables.

- Et encore une fois, nous avons recommandé fortement de prévoir une surveillance et une application indépendantes.

- Le projet de loi 194 rend obligatoire le signalement des atteintes à la vie privée et la tenue d'évaluations de l'impact sur la vie privée; elle prévoit un nouveau régime concernant les plaintes touchant la protection de la vie privée et les enquêtes à leur sujet ainsi que le pouvoir de rendre des ordonnances.

- Nous sommes très favorables à cette réforme, mais nous avons recommandé d'élargir les motifs de plainte et les pouvoirs d'enquête du commissaire, afin de permettre l'inspection sur place des systèmes techniques.

- Enfin, nous avons recommandé d'entamer une refonte de la LAIMPVP dans les plus brefs délais afin que les changements apportés à la LAIPVP y soient inclus. Depuis des décennies, ces deux projets de loi apparentés assurent une protection équivalente

de la vie privée des citoyens dans les institutions provinciales et municipales.

- Renforcer une loi mais pas l'autre donnerait lieu à d'importantes divergences dans les exigences imposées aux institutions provinciales et municipales en matière de protection de la vie privée, ce qui n'aurait aucun sens pour le citoyen moyen.

Conclusion

- Nous sommes à la croisée des chemins. Tout change à un rythme effréné, mais ce changement s'accompagne d'une occasion inouïe de façonner un avenir numérique avantageux pour tous.

- Si le projet de loi C-27 du gouvernement fédéral n'est pas adopté comme prévu, il faudra s'en remettre au projet de loi 194.

- L'Ontario peut faire preuve de leadership dans le monde numérique en adoptant des lois et règlements solides qui protègent la vie privée, stimulent l'innovation et sont adaptés aux circonstances et à la réalité économique uniques de notre province.

- Il est donc d'autant plus crucial de bien faire les choses.

- Dans cette nouvelle ère numérique qui commence, tant le secteur public que le secteur privé doivent privilégier la transparence et la reddition de comptes en amont afin d'assurer la protection de la vie privée et des droits de la personne en aval.

- C'est là une démarche essentielle pour mériter la confiance du public dans l'adoption responsable de technologies et d'approches novatrices qui façonneront un avenir numérique avantageux pour tous, où personne ne sera laissé pour compte.

- Merci.