

**Sous réserve de modifications**

**Allocution de Patricia Kosseim, commissaire à l'information et à la protection de la vie privée de l'Ontario**

**Sommet sur le droit de la protection de la vie privée de l'Association du Barreau de l'Ontario**

**1<sup>er</sup> octobre 2024**

## **Concilier l'innovation de l'IA avec la protection de la vie privée dans le monde numérique d'aujourd'hui**

### **Introduction**

- Bonjour à tous.
- Merci à l'Association du Barreau de l'Ontario de m'avoir invitée, en compagnie de Warren Mar, commissaire adjoint.
- Mes collègues Daniel et Nanditha sont également au kiosque du CIPVP à l'exposition, et je vous invite à passer les voir si vous avez des questions sur notre bureau ou pour obtenir des renseignements et des ressources du CIPVP.
- Je félicite chaleureusement Molly Reynolds, lauréate du prix Karen Spector de cette année. C'est un honneur tout à fait mérité pour ses travaux percutants dans le domaine du droit de la protection de la vie privée, son mentorat au sein du barreau et ses efforts soutenus afin de favoriser la diversité et l'inclusivité en accueillant et en intégrant des membres ayant de l'expérience vécue.
- Les possibilités et les promesses de l'intelligence artificielle (IA) attirent l'attention des médias, des décideurs et des organismes de réglementation du monde entier, sans parler des Ontariennes et des Ontariens dans leur quotidien.
- J'aimerais discuter aujourd'hui de la façon dont nous pouvons adopter l'IA dans le secteur public de façon responsable tout en assurant la protection de la vie privée, la reddition de comptes, la transparence et le respect de l'éthique.
- Je voudrais également vous faire part de ce que nous faisons au CIPVP afin de concrétiser notre vision d'être un organisme de

réglementation moderne et efficace ayant une influence concrète, particulièrement en ce qui concerne l'IA.

### **L'IA dans le secteur public ontarien**

- Les effets positifs des innovations rendues possibles par l'IA sont de plus en plus visibles dans le secteur public.
- De toute évidence, l'IA promet de rehausser l'efficacité, l'efficacité et la réactivité de ce secteur, et d'améliorer les services aux citoyens d'une foule de façons.
- De plus en plus d'agents conversationnels sont mis au point pour répondre plus rapidement aux demandes de renseignements du public, et ils peuvent traduire plusieurs langues en temps réel.
- On utilise des capteurs et des caméras en tenant compte des conditions météorologiques ou de données d'utilisation pour prévoir les besoins des citoyens et déployer les services municipaux plus efficacement (qu'il s'agisse des travaux de voirie, de l'épandage de sel, du déneigement ou de l'enlèvement des ordures).
- Des outils comme ChatGPT sont employés pour faire la synthèse et l'analyse d'une foule de lois et de règlements afin de trouver des réponses préliminaires à des questions, ou pour parcourir les nombreux commentaires recueillis dans le cadre de consultations publiques.
- En Ontario, on a annoncé récemment un projet pilote dans le cadre duquel plus de 150 médecins de premier recours utiliseront des systèmes de transcription numérique fondés sur l'IA. Ces systèmes automatisés résument les entretiens avec les patients pour établir des notes médicales électroniques, permettant ainsi d'alléger le fardeau administratif des médecins, d'améliorer la qualité de leurs interactions avec les patients et de traiter ceux-ci plus rapidement.

- Des institutions publiques utilisent régulièrement des outils d'IA jour et nuit, tous les jours, pour détecter des activités anormales ou douteuses qui pourraient révéler des cybermenaces. Leurs constats sont acheminés à un membre du personnel pour analyse, ce qui peut éviter des attaques contre des infrastructures et services essentiels.

## **Les risques de l'IA**

- Comme toutes les technologies de pointe, l'IA comporte également des risques.
- Faute de surveillance et de réglementation suffisantes, ils peuvent saper les avantages que l'on espère tirer de l'IA.
- Voici des exemples de ses risques pour la vie privée :
  - Il est possible que les données utilisées pour entraîner les systèmes d'IA n'aient pas été recueillies dans le respect de la loi.
  - Ces données sont peut-être fausses ou biaisées, ce qui accroît le risque de conclusions erronées quant à l'employabilité, l'assurabilité ou la solvabilité d'une personne, ou même à son innocence ou à sa culpabilité, et pourrait nuire à son accès à des services de santé ou d'éducation ou à un logement. De pareilles décisions cruciales peuvent bouleverser la vie des gens et exacerber les impacts négatifs sur les groupes vulnérables et historiquement défavorisés.
  - Les outils d'IA peuvent influencer les gens et même les pousser à agir d'une certaine manière, par exemple, les inciter à faire un achat, ou même à dire, croire ou faire certaines choses, ce qui porte atteinte à l'autonomie, à la créativité et à l'intuition humaines.
  - Des personnes ou organisations malveillantes peuvent se servir de l'IA générative pour répandre de la désinformation

dangereuse et créer des hypertrucages à des fins d'exploitation.

- Les attaques d'hameçonnage atteignent un degré de sophistication inégalé grâce aux messages beaucoup plus ciblés et personnalisés que l'IA permet de créer.
- Tout cela sans parler des effets perturbateurs que l'IA pourrait avoir sur le marché du travail et de l'emploi, les droits de propriété intellectuelle et l'environnement, et du risque qu'elle soit employée pour créer des armes biologiques et autonomes, ce qui pourrait avoir des conséquences vraiment catastrophiques.
- Quand on pense aux utilisations actuelles et futures de l'IA dans le secteur public, et que l'on extrapole en partant de ces risques et d'autres encore, on constate que manifestement, sans surveillance adéquate, l'IA pourrait être dangereuse plutôt que prometteuse.

### **Plaidoyer du CIPVP pour une IA responsable**

- Cela nous mène à une importante question : comment favoriser l'innovation plus efficacement tout en assurant le respect du droit à la vie privée?
- Des législateurs du monde entier modernisent leurs lois ou en adoptent de nouvelles pour encadrer l'élaboration ou le déploiement de l'IA au sein des organisations.
- Leur objectif est évidemment de protéger les particuliers contre les préjudices, mais également de favoriser l'acceptation de ces nouvelles technologies dans la société et de susciter la confiance du public dans les organisations qui s'en servent.
- Nous savons aussi que la certitude sur le plan de la réglementation peut stimuler l'innovation en permettant aux organisations, gouvernements et entreprises d'évoluer dans un cadre qui leur procure clarté et confiance.

- Mon bureau encourage l'Ontario à être proactif et à élaborer des lois et politiques provinciales, ou à les mettre à jour, pour répondre à ces besoins.
- L'an dernier, mon bureau a publié une [déclaration commune](#) 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.
- Nous avons dit qu'il est nécessaire d'établir de telles règles pour que l'Ontario puisse profiter pleinement des avantages des technologies de l'IA d'une manière qui soit viable et responsable sur le plan éthique, et qui bénéficie de la confiance du public.
- Conscients de la nécessité d'adopter une approche nationale commune, nous nous sommes joints à nos homologues fédéral, provinciaux et territoriaux pour publier des [Principes pour des technologies de l'IA générative responsables, dignes de confiance et respectueuses de la vie privée](#).
- Ces principes FPT ont pour but d'aider les organisations à intégrer la protection de la vie privée dans la conception des outils d'IA générative et tout au long de leur élaboration, de leur mise à disposition, de leur adoption et de leur utilisation en aval.
- Ces principes visent à atténuer les risques des technologies de l'IA pour la vie privée et à en favoriser la création en toute sécurité.
- Une attention particulière est portée à la protection des groupes vulnérables et historiquement marginalisés, et à la nécessité de faire preuve de la plus grande transparence à leur égard en les informant lorsqu'ils interagissent avec l'IA, ou lorsque les contenus qu'ils consultent ont été créés par un outil d'IA générative.

- Sur la scène internationale, notre bureau et des autorités de protection des données et de la vie privée du monde entier réunis à la [45<sup>e</sup> Assemblée mondiale pour la protection de la vie privée](#) avons souligné la nécessité d'assujettir l'élaboration, le fonctionnement et le déploiement de systèmes d'IA existants et émergents à des principes de base en matière de protection des données et de la vie privée.
- Le CIPVP a coparrainé une résolution sur l'IA en milieu de travail et une autre résolution sur les technologies de l'IA générative.
- Ces deux résolutions ont été adoptées à l'unanimité par des autorités de la protection des données du monde entier et sont dignes d'attention.
- Ces mesures de sensibilisation, entre autres, ont abouti à une recommandation au gouvernement de l'Ontario, dans mon [rapport annuel](#), d'adopter instamment des balises claires et efficaces pour encadrer l'utilisation de l'IA.

### **Projet de loi 194, Loi de 2024 visant à renforcer la cybersécurité et la confiance dans le secteur public**

- En mai 2024, le gouvernement de l'Ontario a déposé le projet de loi 194, [Loi de 2024 visant à renforcer la cybersécurité et la confiance dans le secteur public](#).
- L'annexe 1 du projet de loi vise à réglementer l'utilisation de l'IA par des entités du secteur public, entre autres activités.
- Il est proposé d'établir *par règlement* des exigences en matière de transparence, de reddition de comptes, de gestion des risques, de normes techniques et de surveillance et d'interdire certaines utilisations.

- Bien qu'il s'agisse d'une première étape très importante, mon bureau a déposé un [mémoire](#) à l'Assemblée législative proposant des améliorations à ce projet de loi. Ce mémoire est accessible dans notre site Web.
- Nous recommandons que la loi encadre clairement l'utilisation des technologies de l'IA, pour éviter d'attendre que ces questions fondamentales soient définies plus tard par règlement.
- Nous recommandons également que les outils d'IA qui sont élaborés et déployés présentent les caractéristiques suivantes :
  - **Validité et fiabilité** : Il s'agit là de qualités fondamentales d'outils d'IA dignes de confiance. Il serait irresponsable d'utiliser une technologie de l'IA dont les extrants ne sont pas valables et fiables aux fins pour lesquelles cette technologie a été conçue, utilisée ou mise en œuvre.
  - **Sécurité** : Les systèmes d'IA doivent être conçus pour être favorables à la vie humaine, à la santé physique et mentale, à la sécurité économique et à l'environnement, et faire l'objet d'une surveillance humaine et de mesures de cybersécurité rigoureuses pour en assurer la sécurité.
  - **Protection de la vie privée** : Les technologies d'IA doivent être élaborées et adoptées selon une approche fondée sur la protection intégrée de la vie privée. Les institutions doivent intégrer dans ces technologies des mesures de protection de la vie privée et de sécurité et veiller à ce qu'elles permettent de respecter le droit à l'information.
  - **Transparence** : Il faut adopter des politiques et des pratiques qui rendent visible et compréhensible le fonctionnement d'un outil d'IA. Les institutions doivent privilégier la traçabilité et l'explicabilité.

- **Reddition de comptes** : Les entités du secteur public doivent mettre en place une structure de gouvernance solide pour l'élaboration, le déploiement, l'utilisation, la réaffectation ou la mise hors service de technologies d'IA. Les décisions pouvant se répercuter sur des particuliers doivent faire l'objet d'un examen humain, et ces entités doivent être soumises à l'examen d'un organisme de surveillance indépendant.
  - **Affirmation des droits de la personne** : Les outils d'IA doivent respecter et affirmer les droits des particuliers et des communautés. Ils doivent viser à lutter contre la discrimination et les préjugés historiques et à y remédier, et favoriser la justice et l'équité.
- Nous avons également recommandé de prévoir dans la loi des utilisations interdites de l'IA.
  - C'est particulièrement important quand il existe un seuil de risque clair, ou un niveau de préjudice, au-delà desquels chacun considère que nous ne devrions pas nous aventurer en tant que société.
  - Une autre recommandation importante est d'adopter une approche réglementaire fondée sur les risques.
  - Selon cette approche, des exigences plus strictes et des mesures de surveillance et d'application plus rigoureuses sont imposées à mesure que le degré de risque ou de préjudice éventuel augmente, afin de susciter la confiance du public dans l'utilisation de l'IA par les pouvoirs publics. Il devrait y avoir des consultations publiques et des contacts avec les groupes touchés pour s'assurer que l'IA est au service de *toute* la population ontarienne et profite à tous.
  - Ces recommandations vont généralement dans le sens de plusieurs autres lois adoptées dans le monde, par exemple, la [Législation sur l'intelligence artificielle de l'Union européenne](#), [les mesures de protection des consommateurs du Colorado en lien avec l'intelligence artificielle](#) et la [Loi sur l'intelligence artificielle et les données](#) du

Canada, incluse dans le projet de loi C-27. Aucune de ces lois ne s'appliquerait au secteur public de l'Ontario, d'où la nécessité urgente du projet de loi 194.

- Cela dit, dans le monde numérique en évolution rapide où nous vivons, nous devons adopter une approche qui s'harmonise avec les autres régimes réglementaires nationaux et internationaux, afin d'éviter un amalgame de réglementations diverses au sein des régions, des pays, voire même des provinces.
- De nos jours, bien des gens dans les entreprises et le secteur public hésitent à intégrer ou à utiliser des outils d'IA en raison de cette incertitude sur le plan réglementaire.
- Les institutions du secteur public ne comprennent peut-être pas bien non plus comment collaborer avec le secteur privé pour intégrer ces outils dans leurs programmes et dans la prestation de leurs services.
- Ces préoccupations peuvent causer une réticence à innover. Cette réticence peut aboutir à une stagnation qui défavorise les Ontariennes et les Ontariens.
- Un cadre réglementaire solide peut mener à une plus grande clarté sur l'utilisation responsable de l'IA et favoriser l'innovation multisectorielle de même que la confiance du public.

### **Demandes concernant l'IA dont notre tribunal a été saisi**

- En plus de notre travail sur le plan des politiques, nous avons également commencé à aborder des applications précises de l'IA dans nos enquêtes sur la protection de la vie privée.
- Ainsi, en mars dernier, mon bureau a mené une [enquête](#) sur l'utilisation d'un logiciel de surveillance d'examens utilisant l'IA à l'Université McMaster.

- Nous avons analysé la mesure dans laquelle l'université respectait la loi, et nous avons recommandé des mesures plus solides pour protéger les renseignements personnels des étudiantes et étudiants et une approche qui concilie l'intégrité universitaire avec le respect des droits de ces derniers en matière de protection de la vie privée.
- Nous avons aussi formulé des recommandations visant à atténuer les risques généraux pour la protection de la vie privée et l'éthique qui sont associés à l'utilisation de l'IA par l'université, que celle-ci s'emploie à appliquer.
- Vous trouverez également notre [rapport d'enquête](#) (en anglais) dans notre site Web.

### **Initiatives d'information du public**

- Nous avons également intensifié nos activités d'information du public concernant l'IA, afin d'éclairer la population ontarienne sur les risques et les avantages de l'IA et en quelque sorte élargir le débat en cours dans la société.
- Par exemple, en janvier, à l'occasion de la [Journée de la protection des données](#), nous avons tenu un panel d'experts d'universités, du secteur de la recherche, du monde des affaires, du secteur public et de la société civile pour discuter de l'intelligence artificielle dans le secteur public. Vous pouvez le regarder sur la [chaîne](#) YouTube du CIPVP.
- Nous avons également consacré plusieurs [épisodes](#) de notre balado *L'info, ça compte* à l'IA, dans les secteurs de la santé et du maintien de l'ordre. Je vous invite à les écouter sur notre site Web et partout où vous écoutez vos balados.
- J'ai également écrit plusieurs billets de blogue qui traitent plus en profondeur de certaines questions liées à l'IA et à la protection de la vie privée, dont un qui s'appelle [La vie privée et l'humanité à la](#)

[croisée des chemins](#) – dont le sujet est un aspect auquel je reviendrai dans ma conclusion tantôt. Ces billets de blogue sont accessibles dans notre site Web.

- Je voudrais également souligner quelques autres points...

### **Document d'orientation sur le recours à des fournisseurs externes**

- De plus en plus d'institutions du secteur public confient le traitement de leurs données à des fournisseurs externes, et font appel à eux également pour acquérir des solutions d'IA.
- Notre bureau a publié récemment un document d'orientation sur les [contrats avec des fournisseurs externes](#) qui traite des aspects touchant la protection de la vie privée et l'accès à l'information qui sont associés à l'externalisation.
- Ce document a pour but d'aider les organisations à faire preuve de diligence raisonnable lorsqu'elles externalisent le traitement des données, y compris l'utilisation de l'IA, au lieu de tout laisser au hasard ou de s'en remettre aux promesses des fournisseurs.
- Les institutions doivent pouvoir montrer les mesures qu'elles ont prises pour que les aspects touchant la protection de la vie privée et l'accès à l'information soient pris en compte à toutes les étapes du processus d'approvisionnement : planification, appel d'offres, sélection des fournisseurs, négociations et gestion du contrat.
- Comme nous le répétons souvent, les institutions peuvent externaliser le traitement des données, mais elles ne peuvent échapper à leurs obligations.

## **Modernisation du tribunal**

- Sachez également que depuis le 9 septembre, la version révisée du [code de procédure](#) du CIPVP pour les appels interjetés en vertu de la LAIPVP et de la LAIMPVP est en vigueur.
- Notre code n'avait pas fait l'objet d'une mise à jour importante depuis 1994, alors il était temps!
- Nous avons également mis à jour les directives de pratique et politiques connexes, qui sont accessibles dans notre site Web à [ipc.on.ca/fr](http://ipc.on.ca/fr).
- En tant qu'organisme de réglementation moderne et efficace, le CIPVP tient à bien servir la population ontarienne en traitant les appels de façon juste et équitable, en faisant preuve de transparence quant à ses procédures d'appel, en accélérant le processus et en optimisant l'utilisation des ressources publiques.
- Parmi les modifications apportées au code, mentionnons de nouvelles exigences imposées aux parties qui se servent d'outils d'IA pour préparer leurs observations au CIPVP. Elles doivent maintenant divulguer :
  - le fait que l'IA a été utilisée;
  - le type d'IA qui a été utilisé;
  - comment l'IA a été utilisée.
- En outre, une partie qui utilise des outils d'IA pour préparer des observations à notre bureau doit vérifier l'exactitude et le contenu des références ou analyses juridiques contenues dans ses observations qui sont créées ou générées par l'IA.
- Elle doit aussi attester par écrit au CIPVP qu'elle a procédé à cette vérification.

## L'avenir de l'IA : scénarios plausibles

- Alors, qu'est-ce que l'avenir nous réserve?
- On a beaucoup écrit sur l'avenir de l'IA et ses conséquences, et il est difficile de se retrouver dans tous ces points de vue divers.
- Les perspectives positives ou négatives se succèdent, sans parler des scénarios catastrophiques.
- Du côté des optimistes, voici ce qu'en pense Bill Gates, cofondateur de Microsoft : « L'IA générative a le potentiel de changer le monde d'une manière que nous ne pouvons même pas imaginer. Elle a le pouvoir de créer de nouvelles idées, de nouveaux produits et de nouveaux services qui rendront nos vies plus faciles, plus productives et plus créatives. Elle a également le potentiel de résoudre certains des plus grands problèmes mondiaux, tels que le changement climatique, la pauvreté et la maladie. »
- Pourtant, Bill Gates et d'autres scientifiques et experts de renom dans le domaine de l'IA, y compris deux des trois parrains de l'IA, Geoffrey Hinton et Yoshua Bengio, ont ajouté leur nom à une déclaration commune selon laquelle « l'atténuation du risque d'extinction lié à l'IA devrait être une priorité mondiale au même titre que d'autres risques à l'échelle de la société, tels que les pandémies et les guerres nucléaires ».
- Ils mettent en garde contre une catastrophe menaçant notre existence, et réclament un moratoire mondial sur l'entraînement de l'IA à grande échelle mené par des laboratoires spécialisés « jusqu'à ce que des scientifiques confirment qu'il est sécuritaire de le faire » et trouvent un moyen de faire correspondre les objectifs de l'IA et les valeurs humaines. Ils préconisent une coordination internationale urgente entre les décideurs des pouvoirs publics du monde entier afin d'interdire la création d'une intelligence artificielle générale qui poserait un risque d'extinction de la race humaine.

- En effet, de nombreux scientifiques considèrent qu'il est plausible d'imaginer que des superordinateurs entraîneront l'extinction de l'humanité, comme pourraient le faire le réchauffement planétaire ou les armes nucléaires.
- L'historien et philosophe Yuval Noah Harari compte parmi ceux qui sonnent l'alarme; selon lui, l'IA pourrait signer « la fin de l'histoire humaine – la fin de la période dominée par les êtres humains ».
- De même, Stephen Hawking a prédit un jour : « La création de l'intelligence artificielle serait le plus grand événement de l'histoire de l'humanité. Mais il pourrait aussi être l'ultime. »
- Des cyniques comme Andrew Ng de l'Université Stanford, ancien scientifique en chef chez Baidu, géant chinois d'Internet, considèrent que ces inquiétudes sont très prématurées, comme si « on s'inquiétait de la surpopulation sur Mars ».
- D'autres encore remettent en question ces scénarios effrayants de fin du monde, affirmant qu'ils détournent l'attention des organismes de réglementation des risques bien réels et actuels de l'IA, et qu'en faisant de telles déclarations et en réclamant des moratoires, on crée une forme d'immobilisme réglementaire qui ne contribuera en rien à redistribuer le pouvoir et la richesse concentrés dans les mains des géants de ce secteur.
- Quoi que l'on pense de ces enjeux aujourd'hui, notre opinion évoluera sans doute lorsque nous en saurons plus.
- Comme l'a affirmé avec sagesse Eliezer Yudkowsky, chercheur en IA et fondateur du Machine Intelligence Research Institute : « le plus grand danger de l'intelligence artificielle, et de loin, est de conclure trop tôt qu'on la comprend ».
- Je crois que de toute évidence, nous devons bien réfléchir à la fois aux impacts immédiats et à long terme de l'IA, afin de comprendre dans toute la mesure du possible ses conséquences éventuelles, qu'elles soient positives ou négatives, concrètes ou existentielles,

afin de façonner la destinée que nous souhaitons non seulement pour nous, mais pour les générations futures.

- Comme nous le rappelle Abraham Lincoln, nous ne pouvons pas échapper à la responsabilité de demain en nous déroband à celle d'aujourd'hui.
- Merci.