OSLER

Intelligence artificielle et protection de la vie privée : moments marquants de notre 2e Conférence annuelle à Montréal

Il s’agit du quatrième article d’une série récapitulant la deuxième Conférence annuelle sur la protection de la vie privée à Montréal.

Accéder aux cinq bulletins d’actualités de cette série

19 JANVIER 2026 9 MIN DE LECTURE

Expertises Connexes

- Gestion de risques et réponse aux crises
- Gouvernance d’entreprise
- Intelligence artificielle
- Respect de la vie privée et gestion de l’information
- Technologie

Auteur: François Joli-Coeur

Points à retenir

- Frédérique Horwood a souligné l’essor de l’IA agentive, en mettant en évidence son autonomie par rapport à l’IA traditionnelle.
- Les risques associés à l’IA agentive comprennent notamment les attaques par injection et l’effet de cascade, ce qui exige un déploiement progressif et une surveillance rigoureuse.
- Le cadre de gouvernance de l’IA évolue, avec des responsabilités distinctes pour les développeurs et les utilisateurs selon qu’il s’agisse de solutions B2B ou B2C.

À l’automne, le bureau de Montréal d’Osler a accueilli la deuxième Conférence annuelle sur la protection de la vie privée, organisée par le groupe Respect de la vie privée et gestion de l’information. Cette demi-journée, suivie d’un lunch de réseautage, a réuni des experts du secteur et des juristes d’entreprise pour explorer les enjeux actuels : mise en œuvre des amendements proposés par la Loi 25, tendances récentes en litige, gouvernance de l’intelligence artificielle (IA), technologies émergentes et cybersécurité.

L’un des moments marquants de l’événement a été la discussion entre François Joli-Coeur, associé au sein du groupe national Respect de la vie privée et gestion de l’information, et Frédérique Horwood, conseillère principale, Vie privée et réglementation IA chez Cohere. Les points suivants résument les enseignements clés de leur discussion et proposent des perspectives utiles aux entreprises canadiennes.

Frédérique Horwood : une experte qui travaille quotidiennement

OSLER

à l’intersection de l’IA et de la protection de la vie privée

Enjeux de vie privée liés à l’IA agentive

En abordant le sujet très actuel de l’« IA agentive », Frédérique souligne d’entrée de jeu qu’il n’existe à ce jour aucune définition universellement reconnue de ce concept. Elle propose néanmoins une distinction utile permettant de comprendre les enjeux reliés à l’IA agentive :

- L’IA « traditionnelle » exécute des tâches prévisibles, délimitées et répétitives. Par exemple, cela peut inclure remplir automatiquement des gabarits, analyser une série de documents ou suivre une série d’opérations prédéfinies.
- L’IA agentive, en revanche, se caractérise par un degré plus élevé d’autonomie, de mémoire et de capacité d’adaptation. Elle peut comprendre un contexte, en tirer des conclusions, prendre des décisions, initier des actions de manière proactive et ajuster son comportement au fil du temps. Il s’agit d’une forme d’IA plus dynamique, capable de fonctionner comme un collaborateur numérique.

Risques principaux

L’IA agentive amène de nouveaux risques pour les entreprises[1]. Deux risques principaux liés à l’utilisation de l’IA agentive ont été discutés :

- Attaques par injection (*prompt injection*) : des instructions malveillantes incluses dans des requêtes soumises à un agent ou dans la « mémoire » ou le contexte utilisé par un agent IA peuvent modifier le comportement de celui-ci.
- Effet de cascade (*cascading failure*) : **l’IA agentive amplifie la surface** de risque de manière générale, car les agents sont souvent interconnectés à plusieurs systèmes, ce qui peut entraîner un effet cascade en cas de défaillance ou d’attaque malveillante.

En somme, si l’IA agentive offre la possibilité de gains d’efficacité, elle requiert également une **réflexion approfondie** sur la façon dont ces outils sont déployés, supervisés et intégrés dans les processus opérationnels d’une entreprise.

Exemples d’utilisation d’outils d’IA agentive au sein des services juridiques en entreprise

Certains outils d’IA agentive peuvent être utiles pour les services juridiques des entreprises. Par exemple, ils peuvent aider aux tâches suivantes :

- Automatisation de la révision contractuelle ou de la vérification diligente
- Triage et classification de courriels
- Création automatisée de tableaux de bord et de rapports

Frédérique a également sondé les participants afin de déterminer si leurs organisations avaient commencé à mettre en place de tels agents, par exemple pour réaliser des évaluations des facteurs relatifs à la vie privée (EFVP) ou réviser des ententes de protection des renseignements personnels (DPA). Le faible nombre de réponses affirmatives l’a amenée à constater que, bien que ces outils gagnent rapidement en popularité dans les organisations axées sur l’IA au Canada et aux États-Unis, leur adoption demeure encore limitée dans plusieurs autres secteurs au Canada.

Gouvernance de l'IA : rôles et responsabilités des différents acteurs

Lorsqu'interrogée sur la répartition des responsabilités entre les acteurs de l'écosystème de l'IA, Frédérique distingue deux grandes catégories :

- Développeurs et fournisseurs : les organisations qui conçoivent des modèles de fondation (*foundation models*), des modèles spécialisés ou des infrastructures technologiques permettant la création et la distribution des systèmes d'IA. Ils jouent un rôle déterminant en ce qui concerne la qualité et la provenance des données d'entraînement d'un système d'IA, ainsi que la conception de mécanismes de sécurité intégrés (*built-in safeguards*). Les développeurs et les fournisseurs assurent également une transparence adéquate, incluant la documentation technique et les déclarations reliées aux limites d'un système d'IA.

Utilisateurs et acheteurs : les organisations qui intègrent et déploient des outils d'IA dans leurs environnements opérationnels, qu'il s'agisse d'agents conversationnels, d'outils analytiques ou de systèmes décisionnels. Ils sont principalement responsables de la configuration et la personnalisation du système d'IA, ainsi que de la gestion des renseignements qu'ils fournissent à un système d'IA (par ex. les renseignements inclus dans une requête soumise à un agent conversationnel). Les utilisateurs et acheteurs sont également responsables de l'établissement de contrôles internes et de mécanismes de supervision, ainsi que de l'évaluation des impacts sur la vie privée, la sécurité et l'équité.

Le contexte d'affaires peut influencer fortement les attentes en matière de gouvernance.

- Les solutions B2B (entreprises) : les obligations des parties sont généralement structurées par des ententes commerciales détaillées, comportant des clauses de gouvernance, d'audit, de sécurité, de gestion du cycle de vie des modèles d'IA et de responsabilité contractuelle. Bien qu'elles soient informées par le cadre réglementaire, ces ententes vont souvent au-delà des obligations réglementaires minimales.
- Les solutions B2C (consommateurs) : Comme le rapport entre les parties est différent et les utilisateurs ont rarement l'occasion de négocier leurs ententes, le cadre réglementaire et les normes de protections des consommateurs fournissent souvent les balises principales pour ces solutions. Les fournisseurs comme les acheteurs peuvent être soumis à des attentes réglementaires et à des attentes sociales plus élevées, notamment en matière de transparence, de protection des renseignements personnels, d'équité et de gestion des risques pour les personnes individuelles.

À l'heure actuelle, les **cadres de gouvernance internationaux** (comme la *Loi européenne sur l'intelligence artificielle* ou lignes directrices du National Institute of Standards and Technology [NIST]) se concentrent principalement sur les systèmes d'IA dits **à haut risque** (par ex. ceux utilisés en santé, en éducation, pour le recrutement ou pour l'administration de la justice). Cela signifie que la majorité des cas d'usage d'entreprise, souvent considérés comme « risque faible à modéré », demeurent assujettis à une surveillance réglementaire plus limitée.

Toutefois, il s'agit d'un **paysage en évolution rapide** et il est probable que les législateurs et

OSLER

autorités réglementaires précisent ou élargissent leur champ de surveillance selon les cas de figure d'utilisation de l'IA qui se présenteront.

Standardisation et réglementation mondiale

L'environnement réglementaire de l'IA demeure marqué par une absence d'harmonisation internationale et la difficulté pour certaines régions de concilier innovation et gestion du risque, entraînant parfois des reculs législatifs. Dans cette perspective, la Commission européenne a récemment publié la *Proposition de règlement omnibus numérique sur l'IA*, qui vise à introduire « des mesures de simplification ciblées afin de garantir une mise en œuvre rapide, harmonieuse et proportionnée de certaines dispositions de la législation sur l'IA ». Si elles étaient adoptées, ces mesures repousseraient notamment l'entrée en vigueur de certaines obligations de la *Loi européenne sur l'intelligence artificielle* applicables aux systèmes d'IA à haut risque, à partir de 2027, et, dans certains cas, à 2028.

En Asie-Pacifique, le Japon et la Corée du Sud adoptent des lois multifonctionnelles intégrant sécurité, innovation, investissement économique et formation. L'objectif principal de ces pays est de favoriser une adoption responsable de l'IA tout en renforçant la compétitivité mondiale.

À l'heure actuelle, le Canada ne dispose pas d'un cadre législatif dédié à l'IA. Les priorités du gouvernement canadien visent davantage une adoption responsable qu'une réglementation restrictive.

Le ministère fédéral de l'Intelligence artificielle et de l'Innovation numérique prévoit une réforme du cadre canadien de protection de la vie privée, en modernisant la *Loi sur la protection des renseignements personnels et les documents électroniques* (LPRPDE). Cette réforme ne comprendrait pas de régime réglementaire spécifique à l'IA, à la différence de la *Loi sur l'intelligence artificielle et les données* proposée dans le précédent projet de loi C-27, qui est mort au feuilleton à la fin du mandat du gouvernement précédent.

En parallèle, Innovation, Sciences et Développement économique Canada (ISDE) a récemment mis en place un Groupe de travail sur la stratégie en matière d'IA et lancé une consultation publique en vue d'élaborer la prochaine stratégie canadienne en intelligence artificielle.

Dans le cadre de cette consultation, Osler, via sa plateforme AccessPrivacy, a organisé un atelier vidéoconférence auquel ont assisté deux membres du Groupe de travail dédiés au volet sécurité et confiance du public : Joëlle Pineau, directrice de l'intelligence artificielle (IA), Cohere, et Doyin Adeyemi, candidate au J.D./MBA, Université de Toronto, Fellow 1834. L'enregistrement de cet atelier, qu'il est possible de visionner ici, a été transmis au ministère.

Conclusion : vers une gouvernance intégrée IA-vie privée

Les échanges avec Frédérique confirment que les avancées en intelligence artificielle, les enjeux juridiques liés à la protection de la vie privée et le positionnement stratégique des entreprises sont intimement liés.

Pour gérer efficacement ces trois piliers au sein d'une organisation, les équipes juridiques devraient se tenir à jour des nouvelles technologies et de la façon dont elles sont utilisées au sein de leur entreprise. Il est important de suivre de près l'évolution des cadres réglementaires applicables à l'IA et à la protection des renseignements personnels, incluant dans les territoires situés hors du Canada. Les organisations doivent structurer leur approche d’atténuation de risques autour de trois axes clés : préparation, coordination et gouvernance.

> L’adoption de l’IA doit s’accompagner d’une gouvernance solide : c’est ainsi que les organisations préserveront la confiance et maîtriseront les risques émergents.
>
> *Frédérique Horwood*

---

[1] Voir, par exemple, OWASP Top 10 for Agentic Applications for 2026.