Organismes canadiens de réglementation en assurance

# Préparation à la cybersécurité dans l'utilisation de l'intelligence artificielle générative

## Préambule

Les intermédiaires en assurance réglementés (les « intermédiaires ») ont accès à diverses solutions technologiques sur lesquelles ils s'appuient pour les besoins de la vente ou du service après-vente de produits d'assurance. Certaines d'entre elles reposent sur l'intelligence artificielle générative (l'« IA générative »).

L'IA générative sert à générer du contenu, notamment rédiger ou traduire des textes. Les intermédiaires ont accès à divers programmes ou diverses plateformes ou applications qui y font appel.

Les intermédiaires qui ont recours à des solutions technologiques exploitant l'IA générative (les « solutions d'IA ») dans le cours de leurs activités devraient revoir leurs pratiques de cybersécurité et veiller à mettre en place des mesures adéquates afin de prévenir les cyberincidents susceptibles de compromettre les renseignements sur les clients ou de mener à leur vol.

Le présent document fournit aux intermédiaires de l'information d'ordre général sur l'importance d'adapter leur stratégie de cybersécurité aux risques propres à l'utilisation de solutions d'IA. L'information qui s'y trouve est complémentaire aux pratiques de cybersécurité proposées dans le document intitulé Préparation à la cybersécurité, que les intermédiaires sont invités à consulter.

## Types de solutions d'IA

Les intermédiaires ont accès à diverses solutions d'IA qui sont offertes en ligne ou qui peuvent être intégrées aux systèmes informatiques ou aux réseaux d'une organisation.

**Les solutions publiques et ouvertes** sont accessibles en ligne à tous. L'information partagée par leur entremise est transmise aux fins de traitement à des serveurs qui ne sont pas contrôlés par l'organisation. Elle est ensuite analysée et peut être redistribuée au public. L'organisation n'exerce aucun contrôle sur l'information saisie dans une telle solution, **par exemple, un robot conversationnel accessible gratuitement ou un outil de traduction par abonnement payant.**

**Les solutions sur réseau privé et fermé** sont intégrées au réseau de l'organisation. L'information saisie dans les systèmes informatiques de celle-ci est transmise aux fins de traitement à des serveurs qu'elle ou un tiers fournisseur de services contrôle. Cette information est ensuite analysée et redistribuée uniquement aux utilisateurs autorisés par l'organisation, laquelle peut déterminer les mesures de cybersécurité nécessaires pour prévenir ou atténuer les cyberrisques associés à pareilles solutions. **Un assistant virtuel intégré à un logiciel ou à un service infonuagique en est un exemple.**

**L'IA d'entreprise** est développée par l'organisation ou en collaboration avec un tiers fournisseur de services afin de répondre à des besoins précis. L'information est saisie dans les systèmes informatiques de l'organisation et ensuite traitée sur des serveurs que celle-ci contrôle. L'organisation peut déterminer les mesures de cybersécurité nécessaires pour prévenir ou atténuer les cyberrisques associés à de telles solutions.

# Questions pour les organisations qui utilisent l'IA générative

## 1. Votre organisation utilise-t-elle ou compte-t-elle utiliser l'IA générative?

L'organisation devrait veiller à ce que ses membres ainsi que le responsable de la surveillance des risques de cybersécurité soient en mesure de reconnaître les cas où les solutions technologiques utilisées ou envisagées reposent sur l'IA générative.

Elle devrait connaître les plateformes, les applications et les programmes employés dans le cours de ses activités qui constituent des solutions d'IA ainsi que l'information qui est partagée avec ceux-ci.

L'organisation devrait songer à faire appel à un professionnel en matière de cybersécurité pour comprendre et évaluer les risques rattachés à chaque type de solution d'IA utilisée ou envisagée.

## 2. Connaissez-vous les risques associés à l'IA générative?

L'organisation devrait veiller à mettre en œuvre des mesures de cybersécurité appropriées et à les adapter aux risques propres à chaque type de solution d'IA.

Par exemple, puisque l'information partagée avec une solution publique et ouverte est traitée par des serveurs dont l'organisation n'a pas le contrôle, aucun renseignement confidentiel ne devrait y être saisi.

L'organisation étant responsable des services qu'elle impartit à des tiers fournisseurs de services, elle devrait identifier les risques associés à l'utilisation des solutions d'IA de ces derniers et évaluer leurs pratiques en matière de cybersécurité avant leur intégration à ses systèmes informatiques et réseaux.

## 3. Vos politiques et procédures en matière de cybersécurité sont-elles adaptées à l'utilisation de solutions d'IA?

L'organisation devrait réviser ses politiques et procédures en matière de cybersécurité afin de veiller à ce que ses membres adoptent des pratiques sur le sujet qui conviennent à l'utilisation de solutions d'IA.

À titre d'illustration, elle devrait informer ses membres des solutions d'IA qu'ils sont autorisés à utiliser, interdire le partage de renseignements confidentiels avec une solution publique et ouverte et revoir le contrôle de l'accès aux données saisies dans une solution privée et fermée ou sur mesure.

L'organisation devrait actualiser en conséquence le plan d'intervention en cas de cyberincident.

## 4. Les membres de votre organisation savent-ils comment utiliser l'IA générative en appliquant les pratiques exemplaires en matière de cybersécurité?

L'organisation devrait offrir de la formation et de la sensibilisation continues à ses membres sur les pratiques exemplaires en matière de cybersécurité qui sont propres à l'utilisation de solutions d'IA afin que ceux-ci :

- connaissent les risques associés à l'utilisation de pareilles solutions;
- reconnaissent les cybermenaces connexes;
- suivent les politiques et les procédures établies par l'organisation.

### 5. Avez-vous évalué les conséquences de l'utilisation de l'IA générative sur votre responsabilité?

L'organisation devrait comprendre les conséquences de l'utilisation de solutions d'IA sur sa responsabilité, surtout en cas d'erreur dans le contenu généré par l'une d'elles. Elle devrait consulter un conseiller juridique, au besoin.

L'organisation devrait se doter de contrôles qui évoluent en fonction du recours à ces solutions, notamment en sensibilisant ses membres à l'importance de vérifier le contenu généré avant son utilisation ou sa diffusion.

## Questions pour les personnes qui utilisent l'IA générative

### 1. Votre organisation encadre-t-elle l'utilisation de l'IA générative?

Vérifiez auprès de votre organisation si elle autorise l'utilisation de solutions d'IA.

Prenez connaissance des politiques et procédures de l'organisation sur le sujet et adoptez les pratiques qui y sont établies.

### 2. Savez-vous comment utiliser l'IA générative?

Assistez à des formations qui vous permettront de comprendre le fonctionnement des solutions d'IA et de connaître les risques liés à leur utilisation.

### 3. Savez-vous quelle solution d'IA utiliser?

N'optez que pour les solutions d'IA qui sont autorisées par votre organisation.

Vérifiez auprès de votre organisation avant d'utiliser une solution publique et ouverte; il se peut que vous n'y soyez pas autorisé ou que vous deviez suivre des mesures de cybersécurité pour le faire.

### 4. Savez-vous quelles informations vous pouvez partager avec une solution d'IA?

Respectez les politiques et procédures de votre organisation concernant la collecte, l'utilisation et le stockage des renseignements confidentiels en lien avec de telles solutions.

Ne partagez pas de renseignements confidentiels avec des solutions publiques et ouvertes.

### 5. Puis-je me fier au contenu généré par une solution d'IA?

Le contenu généré par ce type de solution peut comporter des erreurs ou des inexactitudes.

Vérifiez de façon systématique le contenu ainsi généré avant de le communiquer à une autre personne, par exemple un client, et, au besoin, apportez les corrections appropriées.