DÉVELOPPEMENT, OFFRE ET UTILISATION DE TECHNOLOGIES D'IA GÉNÉRATIVE : L'AVIS DES AUTORITÉS CANADIENNES DE PROTECTION DE LA VIE PRIVÉE

Publié le 8 janvier, 2024

Catégories: Perspectives, Publications

Les autorités fédérales, provinciales et territoriales responsables de la protection de la vie privée au Canada ont copublié le document Principes pour des technologies de l'intelligence artificielle (IA) générative responsables, dignes de confiance et respectueuses de la vie privée (les « **Principes** »), où figurent des conseils essentiels pour les organisations qui développent, offrent ou utilisent des systèmes d'intelligence artificielle générative (« **IA générative** »).

Capable de produire des textes, des images ou des contenus audio en réponse à une requête utilisateur, l'IA générative, une catégorie de technologies d'apprentissage machine, a le vent dans les voiles. Cependant, son recours à de vastes ensembles de données d'entraînement et à une multitude d'intrants d'utilisateurs, qui comprennent souvent des renseignements personnels, occasionne des difficultés particulières sur le plan de la protection de la vie privée.

Les Principes s'adressent aux organisations assujetties aux lois sur la protection de la vie privée dans le secteur public, le secteur privé et le domaine de la santé au Canada. Quoique présentés comme des recommandations, les points qui y sont soulevés feront dans bien des cas naître des obligations de conformité aux lois sur la protection de la vie privée pour les organisations.

Le présent bulletin résume les éléments applicables aux organisations qui développent, offrent ou utilisent des systèmes d'IA générative. Il est cependant conseillé de consulter les Principes dans leur intégralité, car ils contiennent des recommandations supplémentaires, dont certaines concernent exclusivement les développeurs, les fournisseurs ou les utilisateurs.

Grands principes et recommandations

Selon les autorités canadiennes de protection de la vie privée, dix grands principes de protection de la vie privée s'appliquent au développement, à l'offre et à l'utilisation de systèmes d'IA générative :

1. **Pouvoir légal et consentement**

L'organisation doit documenter les assises juridiques lui permettant de recueillir, d'utiliser, de communiquer et de détruire des renseignements personnels dans le cadre de l'entraînement, du développement, du déploiement, de l'exploitation ou de la mise hors service d'un système d'IA générative. Les Principes indiquent que le recours à l'IA générative pour inférer des renseignements sur une personne identifiable constitue une « collecte » de renseignements personnels et, par conséquent, requiert un consentement ou une autre assise juridique.

Lorsque le consentement est l'assise juridique, l'organisation doit s'assurer qu'il est précis, « valide et valable » et qu'il n'a pas été obtenu au moyen de pratiques trompeuses.

Si elle obtient des renseignements personnels auprès d'un tiers dans le cadre du recours à un système d'IA générative, l'organisation doit s'assurer que le tiers les a recueillis légalement et est juridiquement habilité à les communiquer.

2. Fins appropriées

L'organisation doit éviter de recueillir, d'utiliser ou de communiquer des renseignements personnels à des fins inappropriées et déterminer si le recours à un système d'IA générative convient à une application spécifique. Elle doit, entre autres, se garder de développer, de mettre en service ou d'utiliser des systèmes d'IA générative qui violent des « zones interdites » déjà établies par les autorités canadiennes de protection de la vie privée (p. ex., profilage discriminatoire, production de contenus brimant un droit fondamental) ou des zones interdites émergentes potentielles figurant dans les Principes (p. ex., création de contenus à des fins malveillantes, y compris par hypertrucage).

3. Nécessité et proportionnalité

L'organisation doit établir qu'il est nécessaire d'utiliser l'IA générative et les renseignements personnels dans les systèmes d'IA générative pour atteindre les objectifs et dans quelle proportion cette utilisation est justifiée. Les Principes recommandent, autant que possible, d'utiliser dans les systèmes d'IA générative des données anonymisées, synthétiques ou dépersonnalisées plutôt que des renseignements personnels.

4. Transparence

L'organisation doit, tout au long du développement, de l'entraînement et de l'exploitation des systèmes d'IA générative dont elle est responsable, se montrer transparente quant à la collecte, à l'utilisation et à la communication des renseignements personnels et aux risques liés à la protection de la vie privée des personnes. Elle doit notamment énoncer en toutes lettres les fins appropriées de la collecte, de l'utilisation ou de la communication et indiquer clairement, lorsque les extrants sont susceptibles d'avoir une incidence importante sur un individu ou un groupe, qu'ils sont issus d'un outil d'IA générative. Les informations en

question doivent être facilement accessibles avant, pendant et après l'utilisation du système d'IA générative.

5. Responsabilité

Il convient d'établir une structure de gouvernance interne robuste afin d'assurer la conformité aux lois sur la protection de la vie privée, y compris les rôles et les responsabilités, les politiques et les pratiques définis qui établissent des attentes claires en ce qui concerne la conformité aux obligations en la matière, ainsi que de s'engager à revoir régulièrement les mesures de responsabilisation (y compris les évaluations des biais) à mesure que les technologies et la réglementation évoluent. Les Principes recommandent par ailleurs la réalisation d'évaluations des facteurs relatifs à la vie privée ou de l'incidence algorithmique afin de cerner et d'atténuer les répercussions potentielles ou connues que le système d'IA générative (ou son utilisation) peut avoir sur la protection de la vie privée ou d'autres droits fondamentaux.

6. Accès aux renseignements personnels

Les Principes accordent une grande importance au droit des personnes d'accéder aux renseignements personnels qui sont recueillis à leur sujet au moyen d'un système d'IA générative ou qui sont contenus dans un modèle d'IA générative, ainsi qu'à leur droit de corriger ces renseignements. L'organisation doit disposer de procédures permettant aux personnes d'exercer ces droits.

7. Limitation de la collecte, de l'utilisation et de la communication des renseignements

L'organisation doit limiter la collecte, l'utilisation et la communication des renseignements personnels à ce qui est nécessaire aux fins appropriées dûment définies. Les Principes précisent que les renseignements personnels accessibles au public (dont les renseignements personnels publiés en ligne) ne peuvent pas être recueillis ou utilisés sans discernement, y compris pour les besoins d'un système d'IA générative. Les renseignements personnels contenus dans les données d'entraînement, les requêtes et les extrants d'un système d'IA générative doivent faire l'objet de calendriers de conservation appropriés.

8. Exactitude

Les renseignements personnels utilisés dans le cadre du recours à un système d'IA générative doivent être aussi exacts, complets et à jour que ce qui est nécessaire aux fins de cette utilisation. Il faut notamment porter à l'attention des utilisateurs d'un système d'IA générative les limites ou problèmes connus quant à l'exactitude des extrants du système et prendre des mesures raisonnables pour s'assurer que l'exactitude de ces extrants est suffisante en ce qui concerne la fin prévue, en particulier si les extrants seront utilisés pour prendre (ou éclairer) des décisions au sujet d'une ou plusieurs personnes, seront employés dans un contexte à risque élevé ou seront rendus publics.

9. Mesures de protection

Il convient d'établir des mesures pour protéger les renseignements personnels recueillis ou utilisés tout au long du cycle de vie d'un système d'IA générative contre les risques d'utilisations inappropriées et d'atteintes à la sécurité. Les mesures de protection doivent être en adéquation avec le caractère sensible des renseignements personnels et tenir compte des risques propres aux systèmes d'IA générative, dont les attaques par injection de requêtes, les attaques par inversion de modèle et le débridage.

10. Incidence sur les groupes vulnérables

L'organisation qui développe ou déploie un système d'IA générative doit cerner et prévenir les risques pour les groupes vulnérables, dont les enfants et les populations ayant historiquement vécu de la discrimination ou les conséquences de biais. Les systèmes d'IA générative doivent être équitables et exempts de biais pouvant se solder par des résultats discriminatoires. À ce titre, les développeurs doivent notamment veiller à ce que les ensembles de données d'entraînement ne viennent pas reproduire ou renforcer les biais historiques ou actuels ou en introduire de nouveaux.

Les utilisateurs doivent superviser et examiner les extrants et vérifier s'il y a des effets négatifs potentiels, surtout s'il est prévu d'utiliser les extrants dans le cadre d'un processus décisionnel administratif ou dans un contexte aux incidences élevées (p. ex., emploi, soins de santé, accès au financement).

Autres nouveautés concernant le projet de règlement canadien sur l'intelligence artificielle

La publication des Principes fait écho à un mouvement mondial appelant à la prudence et à la responsabilité vis-à-vis du développement et de l'utilisation de l'intelligence artificielle (« **IA** »).

Le Canada et les États-Unis (entre autres pays) ont adopté les Lignes directrices pour le développement de systèmes d'IA sécurisés[1], qui recommandent que les systèmes d'IA soient conçus, développés, déployés et exploités de façon transparente et sûre. Cette collaboration internationale est signe d'une approche unifiée de la part d'un certain nombre d'organismes gouvernementaux quant à l'atténuation des risques que peuvent comporter les technologies d'IA.

Autre avancée majeure vers l'adoption responsable de ces technologies, plusieurs chefs de file, dont CGI et IBM, ont signé le Code de conduite volontaire visant un développement et une gestion responsables des systèmes d'IA générative avancés du Canada. Cet engagement volontaire de la part d'acteurs importants du domaine de l'IA générative témoigne du consensus grandissant qui entoure l'importance de la sécurité et de l'éthique dans le développement et la gestion des systèmes d'IA.

Enfin, une réforme législative importante concernant les échanges et le commerce internationaux et

interprovinciaux en matière de systèmes d'IA poindrait à l'horizon. S'il est adopté, le projet de loi C-27, toujours à l'étude en comité à la Chambre des communes, formera (avec les changements projetés) la *Loi sur l'intelligence artificielle et les données* (la « **LIAD** »)[2]. La LIAD viendrait codifier une partie des Principes relativement à certaines activités réglementées qui impliquent des systèmes d'IA, dont des obligations ayant trait aux évaluations des risques et à la transparence.

Points importants pour les entreprises

Vu la nature complexe et évolutive des technologies en question, il est primordial pour les organisations qui développent, offrent ou utilisent des systèmes d'IA générative :

- d'analyser en profondeur leurs systèmes d'IA générative actuels et futurs, ainsi que les utilisations qu'ils en font, à l'aune des recommandations énoncées dans les Principes;
- d'instaurer des politiques et procédures robustes de gouvernance des données qui respectent les Principes et les lois sur la protection de la vie privée;
- de mettre en place des mécanismes clairs et complets de consentement à la collecte, à l'utilisation et à la communication de renseignements personnels dans le cadre du recours à un système d'IA générative, à moins qu'il y ait une autre assise juridique pour le traitement des renseignements personnels en question;
- de surveiller et mettre à jour continuellement les systèmes d'IA générative pour remédier aux préoccupations ou biais émergents en matière de protection de la vie privée;
- de favoriser une culture de la protection de la vie privée et du recours éthique à l'IA générative, de sorte que toutes les parties prenantes connaissent leurs responsabilités (p. ex., en suivant des formations propres aux fonctions exercées);
- de collaborer avec des juristes pour s'assurer que leurs initiatives d'IA respectent les lois sur la protection de la vie privée, les Principes et les lignes directrices des autorités canadiennes de protection de la vie privée, ou soient compatibles avec les résultats d'enquête publiés ultérieurement par ces dernières.

Vous avez des questions sur les Principes ou sur l'application des lois canadiennes actuelles et futures en matière de protection de la vie privée au développement, à l'offre ou à l'utilisation de technologies d'IA générative? Les avocats de notre groupe Protection de la vie privée et des données se feront un plaisir de vous aider.

[1] Canada, U.S. sign international guidelines for safe AI development | IT World Canada News.
[2] Voir notre précédent bulletin sur le projet de loi C-27 intitulé « La protection de la vie privée de retour au feuilleton fédéral».

Par Kristen Pennington, Robert C. Piasentin, Robbie Grant et Stephen Johnson (stagiaire en droit)

Mise en garde