CPA COMPTABLES PROFESSIONNELS AGRÉÉS CANADA

Établir un cadre de gestion des risques pour une IA digne de confiance

Janvier 2022

CPA Canada
Voir demain
RÉIMAGINER LA PROFESSION.

22-2315

À PROPOS DE CPA CANADA

Comptables professionnels agréés du Canada (CPA Canada) travaille en collaboration avec les ordres de CPA des provinces, des territoires et des Bermudes, et représente la profession comptable canadienne sur les scènes nationale et internationale. La profession canadienne peut ainsi faire la promotion de pratiques exemplaires, favorables aux entreprises et à la société en général, et préparer ses membres aux défis posés par un contexte en évolution constante, marqué par des changements sans précédent. Forte de plus de 220 000 membres, CPA Canada est l'une des plus grandes organisations comptables nationales au monde. cpacanada.ca

La version électronique de ce document est disponible sur le site **cpacanada.ca**.

© 2022 Comptables professionnels agréés du Canada

Tous droits réservés. Cette publication est protégée par des droits d'auteur et ne peut être reproduite, stockée dans un système de recherche documentaire ou transmise de quelque manière que ce soit (électroniquement, mécaniquement, par photocopie, enregistrement ou toute autre méthode) sans autorisation écrite préalable.

Table des matières

Les prévisions météorologiques, le filtrage des pourriels, les prédictions de recherche de Google et les appareils de reconnaissance vocale, comme Siri d'Apple, sont autant d'exemples de systèmes d'intelligence artificielle (IA) qui apportent une précieuse valeur ajoutée aux entreprises, aux consommateurs et à la société en général.

Les technologies qui utilisent des algorithmes d'apprentissage automatique pour réagir en temps réel sans intervention humaine améliorent déjà la productivité des entreprises, et les perspectives de croissance sont impressionnantes. Selon un sondage mené par la société de conseil en gestion McKinsey, l'analyse reposant sur l'intelligence artificielle pourrait ajouter environ 13 billions de dollars américains ou 16 % au PIB mondial annuel d'ici 2030[1].

1 McKinsey Global Institute. *Notes from the AI Frontier: Modeling the Impact of AI on the World Economy*, septembre 2018, 61 pages. https://www.mckinsey.com/~/media/mckinsey/featured%20insights/artificial%20intelligence/notes%20from%20the%20frontier%20modeling%20the%20impact%20of%20ai%20on%20the%20world%20economy/mgi-notes-from-the-ai-frontier-modeling-the-impact-of-ai-on-the-world-economy-september-2018.pdf?shouldIndex=false

Malgré ces résultats potentiels spectaculaires, le déploiement des systèmes d'IA comporte sa part de risques – des risques dont les organisations en pleine transformation numérique doivent être conscientes. Une utilisation mal intentionnée des systèmes d'IA peut mener à la création d'outils puissants pour des pratiques de manipulation, d'exploitation et de contrôle social. Par conséquent, à la lumière de récents développements – en particulier aux États-Unis et dans l'Union européenne (UE) –, on s'attend à un encadrement de l'utilisation éthique des systèmes d'IA, d'où la nécessité de se doter de cadres de gestion des risques pour orienter le développement, les essais et l'utilisation de l'IA.

Selon Rachel Kirkham, vice-présidente, Analytique et science des données chez MindBridge, « comme de nombreuses données pointent vers la possibilité de préjudices découlant d'une mauvaise utilisation de cette technologie, il est temps de mettre en place des cadres pour gérer celle-ci du point de vue de la réglementation et des risques de l'entreprise[2] ».

Les comptables jouent un rôle dans la collecte, l'analyse, l'interprétation et la communication d'informations aux fins des processus décisionnels qui aident à la fois les parties prenantes internes et externes à comprendre et à influencer les inducteurs de performance. Ils peuvent aussi établir des liens entre le risque et les indicateurs de performance de l'entreprise, en fournissant, grâce aux évaluations des risques, une information pertinente[3]. Ainsi, les CPA sont bien placés pour contribuer à concevoir et à mettre en place des systèmes et des contrôles favorisant une IA digne de confiance.

Le présent guide propose des mesures concrètes pour réaliser des progrès à cet égard.

2 CPA Canada, balado Voir demain. https://www.cpacanada.ca/fr/voir-demain-initiative/voir-demain-balados/technologie-arme-deux-tranchants.

3 CPA Canada et IFAC. Une gestion intégrée du risque organisationnel plutôt qu'autonome, mai 2015. https://www.cpacanada.ca/fr/ressources-en-comptabilite-et-en-affaires/strategie-risque-et-gouvernance/gestion-du-risque-dentreprise/publications/une-gestion-integree-du-risque-organisationnel-plutot-quautonome.

S’attaquer à la montée du déficit de confiance

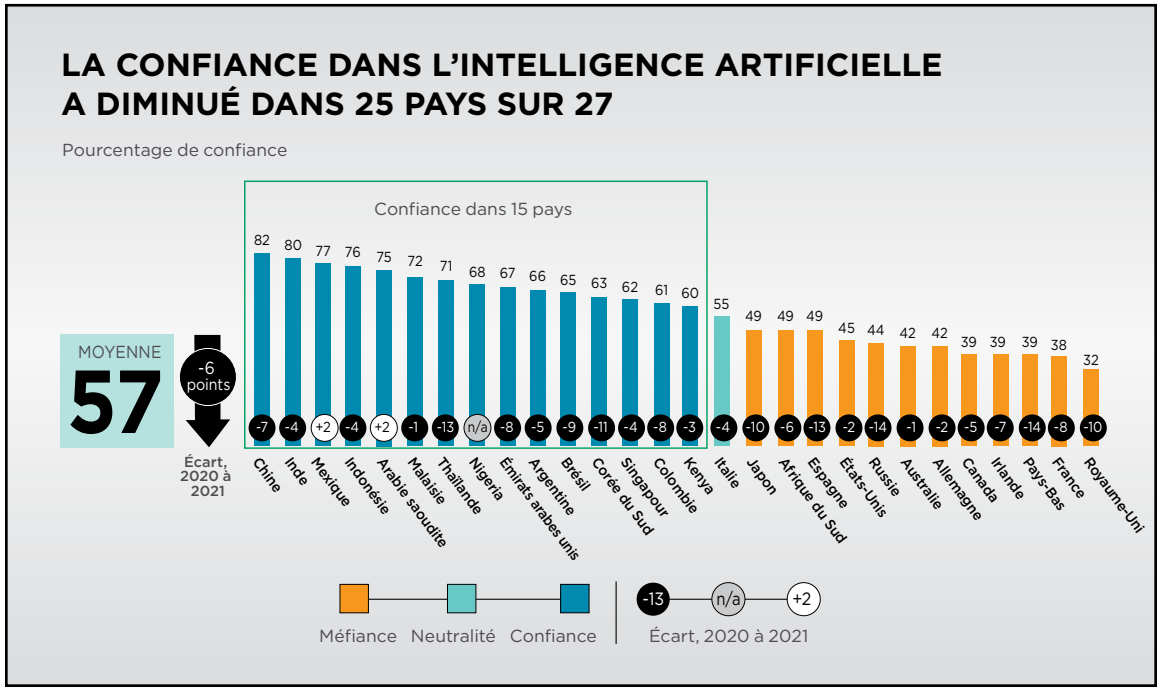
La confiance est la force la plus puissante sur laquelle repose le succès de toutes les entreprises, mais elle peut être anéantie en un rien de temps. Lorsqu’il est question de confiance dans les technologies numériques, tout indique que nous approchons d’un point de rupture. Depuis l’utilisation abusive systémique des données par les grandes plateformes technologiques jusqu’aux fausses nouvelles conçues pour créer la division et le conflit, en passant par les atteintes à la vie privée et les attaques par rançongiciel, le secteur des technologies semble plongé dans une crise de confiance croissante. Les organisations en cours de transformation numérique sont de plus en plus conscientes qu’elles peuvent être touchées par ce déficit de confiance, avec les graves conséquences qui pourraient s’ensuivre. Les préjugés découlant d’ensembles de données biaisés peuvent être intégrés dans les algorithmes, entraînant de mauvaises décisions qui risquent de nuire aux entreprises, à leurs parties prenantes et à la société en général.

« Une fois que le système est au point, il est trop tard pour se poser des questions aussi cruciales que “devrions-nous vraiment construire ce système?” et “comment se prémunir contre les partis pris et garantir l’équité?”. Quand on en est là, le génie est sorti de la bouteille, comme on dit, particulièrement si on découvre le problème d’éthique après avoir investi en développement beaucoup de temps, d’argent et d’énergie créatrice[4]. »

4 CPA Canada, en collaboration avec l’IFAC, l’ICAS et l’IESBA. *La technologie, une arme à double tranchant : Occasions et défis pour la profession comptable*. https://www.cpacanada.ca/fr/voir-demain-initiative/confiance-et-ethique/technologie-arme-double-tranchant.

Dans son Baromètre de confiance de 2021, Edelman, par l'intermédiaire de son sondage annuel auprès de 33 000 personnes dans 27 pays, a constaté que la confiance dans l'IA avait diminué dans 25 pays sur 27[5]. Au Canada, la confiance dans l'IA a diminué de 5 points de pourcentage pour atteindre 39 %. Les consommateurs sont de plus en plus préoccupés par les préjudices que l'IA peut causer aux populations vulnérables en raison de l'opacité, de la complexité, des préjugés, de l'imprévisibilité et des comportements partiellement autonomes de certains systèmes d'IA.

Figure 1



Source : Baromètre de confiance d'Edelman 2021. https://www.edelman.com/sites/g/files/aatuss191/files/2021-03/2021%20Edelman%20Trust%20Barometer%20Tech%20Sector%20Report_0.pdf, p. 44.

5 La méthodologie du sondage mené pour le Baromètre de confiance annuel d'Edelman est accessible à la page 2 ainsi que dans les annexes concernées du rapport de 2021 : https://www.edelman.ca/fr/trust-barometer/edelman-trust-barometer-2021.

« Étant donné l'importance croissante que prend la confiance à l'ère numérique, les leaders – y compris les [professionnels comptables] – font l'objet de grandes attentes sur le plan du comportement responsable et de la reddition de comptes. Les lacunes à cet égard pourraient être perçues comme un manque d'intégrité et de professionnalisme risquant de nous discréditer. »

Extrait de *La technologie, une arme à double tranchant : Occasions et défis pour la profession comptable*; CPA Canada, en collaboration avec l'IFAC, l'ICAS et l'IESBA

Qu'est-ce qu'une IA digne de confiance?

En réponse aux préoccupations relatives à la confiance, les gouvernements, l'industrie et la société civile ont défini de nouvelles approches afin de gérer les risques associés aux systèmes d'IA. Le concept dépassé d'IA éthique, élaboré pour encadrer le déploiement de l'IA, a été remplacé par un cadre plus large visant une IA digne de confiance[6]. Selon William Diab, expert de renommée mondiale en systèmes d'IA qui a contribué à l'élaboration d'une nouvelle norme ISO sur l'IA digne de confiance, « chaque client – qu'il s'agisse d'une société de services financiers, d'un détaillant ou d'un fabricant – se demandera à qui faire confiance. Il faut aborder de nombreux aspects, notamment les préoccupations de la société, comme la qualité des données, la protection des renseignements personnels, les préjugés potentiellement injustes et la sécurité[7]. »

6 Par exemple, de nouveaux règlements encadrant l'IA sont en cours d'élaboration dans l'UE en vertu de la Loi sur l'intelligence artificielle : Proposition de règlement établissant des règles harmonisées concernant l'intelligence artificielle. https://eur-lex.europa.eu/resource.html?uri=cellar:e0649735-a372-11eb-9585-01aa75ed71a1.0020.02/DOC_1&format=PDF. Un nouveau cadre de gestion volontaire des risques pour l'IA est en cours d'élaboration par le National Institute of Standards and Technology en réponse à un décret de la Maison-Blanche. https://www.nist.gov/system/files/documents/2019/08/10/ai_standards_fedengagement_plan_9aug2019.pdf. À l'échelle internationale, de nouvelles normes volontaires sur la fiabilité de l'IA ont été publiées par des organismes comme l'Organisation internationale de normalisation (ISO). https://www.iso.org/fr/standard/77608.html?browse=tc. L'Institute of Electrical and Electronics Engineers (IEEE) est également en train d'élaborer une gamme complète de normes dans sa série 7000, dans le cadre de son initiative de conception éthique (Ethically Aligned Design). Les enjeux abordés vont de la transparence aux processus de protection de la confidentialité des données, en passant par les biais algorithmiques et la gouvernance des données sur les enfants, les étudiants et les employeurs. https://ethicsstandards.org/p7000/. En ce qui concerne les normes volontaires canadiennes régissant la gouvernance numérique, le Conseil stratégique des DPI a publié une norme sur l'IA éthique intitulée « Intelligence artificielle : Conception éthique et utilisation de systèmes de décision automatisés ». https://ciostrategycouncil.com/normes/conception-ethique/?lang=fr.

7 https://www.iso.org/fr/news/ref2530.html

Au fil des ans, on a fait de nombreuses déclarations et attestations sur l'IA éthique et digne de confiance[8]. Actuellement, l'IA digne de confiance incarne généralement les concepts suivants :

- **Exactitude** – L'IA doit prendre les bonnes décisions.
- **Explication** – Le processus décisionnel employé par le système doit être documenté, compris et reproduit par des humains.
- **Résilience** – Lorsque de nouvelles données font en sorte qu'un système d'IA fonctionne à l'extérieur de ses limites nominales, le système doit être en mesure de s'adapter aux nouvelles conditions ou d'alerter les humains afin d'éviter une défaillance catastrophique.
- **Sécurité** – Les systèmes d'IA ne doivent pas créer de risques pour la santé ou la sécurité des personnes ou de l'environnement.
- **Fiabilité** – Les systèmes d'IA doivent être conçus pour fonctionner de façon continue et cohérente.
- **Objectivité** – Les systèmes d'IA doivent être exempts de préjugés ou de biais à l'égard de personnes ou de groupes.
- **Inclusivité en matière de croissance, de développement durable et de bien-être** – Les systèmes d'IA doivent contribuer à produire des résultats bénéfiques pour les gens et la planète, dans le respect de valeurs fondamentales comme les droits démocratiques, l'équité et la protection des renseignements personnels.

8 Parmi les nombreuses déclarations et attestations sur cette question, on note les principes d'Asilomar proposés par le Future of Life Institute https://futureoflife.org/ai-principles/, la Charte internationale sur les données ouvertes https://opendatacharter.net/principles-fr/, la Déclaration de Montréal de 2017 pour un développement responsable de l'intelligence artificielle https://www.declarationmontreal-iaresponsable.com/, les *Top 10 Principles for Ethical Artificial Intelligence* http://www.thefutureworldofwork.org/media/35420/uni_ethical_ai.pdf et l'accord international des États membres de l'UNESCO sur l'éthique de l'intelligence artificielle https://fr.unesco.org/artificial-intelligence/ethics#recommendation.

Trois catégories de systèmes d'IA

Les systèmes d'IA ne sont pas tous identiques. Certains, comme les algorithmes qui proposent des listes de lecture musicale et des suggestions de films par le biais de services de diffusion en continu ou ceux qui font la promotion de produits en générant de la publicité en ligne, peuvent généralement être gérés sans crainte de préjudices graves. En revanche, les systèmes d'IA qui prennent des décisions de vie ou de mort, comme les véhicules autonomes ou les dispositifs de commande d'infrastructures essentielles, exigent un degré élevé de surveillance. Les récents progrès réalisés en Europe laissent entrevoir la segmentation de l'IA selon diverses catégories afin de concentrer les ressources gouvernementales et réglementaires limitées sur les systèmes d'IA à risque élevé. Dans son règlement déposé récemment sur l'IA digne de confiance, la Commission européenne décrit une approche fondée sur les risques modulée en trois catégories de systèmes d'IA. Ces catégories peuvent servir de balises aux organisations qui cherchent à se doter d'une IA digne de confiance.

La première catégorie comprend les **systèmes d'IA à risque élevé « inacceptables »,** qui peuvent contrevenir aux lois ou violer des droits fondamentaux. En voici quelques exemples :

- Les pratiques qui ont le potentiel de manipuler les individus par des techniques subliminales échappant à leur conscience, qui influencent le comportement humain ou qui exploitent des groupes vulnérables tels que les enfants ou les personnes handicapées.
- Les systèmes qui attribuent des pointages sociaux à des personnes ou qui évaluent ou classent la fiabilité des personnes sur la base de leur comportement social.

On s'attend à ce que les systèmes à risque élevé considérés comme inacceptables soient interdits d'utilisation dans l'UE.

La deuxième catégorie comprend les **systèmes d'IA à risque élevé qui peuvent être gérés.** Les systèmes d'IA qui présentent un risque élevé pour la santé et la sécurité ou qui pourraient menacer les libertés et droits fondamentaux entrent dans cette catégorie. En voici des exemples :

- Les systèmes d'IA destinés à être utilisés comme composante de sécurité de produits déjà visés par la réglementation en matière de sécurité publique, dont l'électricité, la plomberie, les appareils sous pression, le matériel de chauffage et de climatisation, les ascenseurs, les jouets, le matériel de sécurité des travailleurs, le matériel radio et l'équipement utilisé dans les environnements dangereux. De plus, on s'attend à ce qu'un large éventail de nouvelles catégories de produits, comme les robots autonomes dans les domaines de la fabrication ainsi que de l'assistance et des soins personnels, ou encore les systèmes de diagnostic et de soins de santé soutenant des décisions médicales fondées sur des systèmes d'IA autonomes sophistiqués, soient incluses.
- Les systèmes qui peuvent avoir un impact sur le droit à la dignité humaine, la vie privée et familiale, la discrimination basée sur des données personnelles ainsi que d'autres droits et libertés. On trouve des systèmes d'IA susceptibles d'avoir une incidence sur les droits et libertés dans une vaste gamme de secteurs, dont les finances, les notations de crédit, l'assurance, l'éducation, la gestion des ressources humaines (dans des fonctions comme le recrutement et l'embauche), l'application de la loi et les procédures administratives, et enfin, l'administration de la justice et les processus démocratiques.

La troisième catégorie comprend tous les autres **systèmes d'IA jugés à faible risque, qui peuvent être déployés sans contraintes sévères.** Les organismes de réglementation recommandent la mise en place de codes de pratiques volontaires pour maintenir la sécurité des systèmes d'IA à faible risque.

Gestion de l'IA à risque élevé

> « Divers risques menacent l'intégrité de l'information durant le cycle de vie de l'information et accroissent la possibilité que des erreurs et des omissions graves dans l'information entraînent des décisions erronées ou peu judicieuses. »
>
> Extrait du *Cadre de contrôle de l'intégrité de l'information* de CPA Canada

Les organisations qui déploient des systèmes d'IA doivent prendre des mesures pour gérer les risques connexes et, par conséquent, mettre en œuvre une IA digne de confiance. Les solutions proposées ci-après sont tirées de récentes initiatives en matière de réglementation et de normes aux États-Unis, en Europe et au Canada[9].

- **Instaurer un cadre de responsabilisation.** Les organisations doivent s'assurer que les systèmes d'IA répondent aux caractéristiques d'une IA digne de confiance tout au long de leur cycle de vie – ce qui peut comprendre l'élaboration, la mise à l'essai, le déploiement, l'exploitation, la mise à niveau et la mise hors service des systèmes d'IA actuels. Il est à

9 Par exemple, de nouveaux règlements encadrant l'IA sont en cours d'élaboration dans l'UE en vertu de la Loi sur l'intelligence artificielle : Proposition de règlement établissant des règles harmonisées concernant l'intelligence artificielle. https://eur-lex.europa.eu/resource.html?uri=cellar:e0649735-a372-11eb-9585-01aa75ed71a1.0020.02/DOC_1&format=PDF. Un nouveau cadre de gestion volontaire des risques pour l'IA est en cours d'élaboration par le National Institute of Standards and Technology en réponse à un décret de la Maison-Blanche. https://www.nist.gov/system/files/documents/2019/08/10/ai_standards_. À l'échelle internationale, de nouvelles normes volontaires sur la fiabilité de l'IA ont été publiées par des organismes comme l'Organisation internationale de normalisation (ISO). https://www.iso.org/fr/standard/77608.html?browse=tc. L'Institute of Electrical and Electronics Engineers (IEEE) est en train d'élaborer une gamme complète de normes dans sa série 7000, dans le cadre de son initiative de conception éthique (Ethically Aligned Design). Les enjeux abordés vont de la transparence aux processus de protection de la confidentialité des données, en passant par les biais algorithmiques et la gouvernance des données sur les enfants, les étudiants et les employeurs. https://www.iso.org/fr/standard/77608.html?browse=tc. En ce qui concerne les normes volontaires canadiennes régissant l'IA et l'apprentissage machine, le Conseil stratégique des DPI travaille à l'élaboration d'une série de normes en matière de gouvernance numérique portant notamment sur l'IA. Parmi les publications d'intérêt récentes, mentionnons la norme « Intelligence artificielle : Conception éthique et utilisation de systèmes de décision automatisés ». https://ciostrategycouncil.com/normes/conception-ethique/?lang=fr.

noter que la nouvelle réglementation de l'UE exigera des organisations qui déploient des systèmes d'IA à risque élevé qu'elles désignent un fournisseur pour gérer ce cadre de responsabilisation.

- **Utiliser les systèmes de gestion de la qualité actuels** pour faire le suivi de l'IA digne de confiance et en rendre compte. La réglementation de l'UE exigera que les organisations mettent en place des systèmes de gestion appropriés, comme la norme ISO 9001, chaque fois que des systèmes d'IA à risque élevé sont mis au point, utilisés ou vendus. En s'engageant à atteindre des objectifs de qualité et d'amélioration continue pour assurer la fiabilité de l'IA grâce à un cadre de gestion de la qualité, les organisations pourront fixer des objectifs, documenter leurs efforts, comparer leur performance à l'échelle des chaînes d'approvisionnement et gérer les risques[10]. Par ailleurs, la performance de l'IA peut être suivie au moyen des processus, des stratégies et des **systèmes de gestion des risques** de l'entreprise. Les risques associés aux systèmes d'IA peuvent être documentés et suivis au moyen d'un système de gestion fondé sur des normes comme ISO 31000[11].
- **Établir des politiques et des procédures pour gérer les systèmes d'IA.** Des procédures sont nécessaires pour favoriser l'obtention d'ensembles de données de haute qualité, la mise à jour de la documentation technique, la tenue de registres et l'archivage des ensembles de données. Il peut être nécessaire de modifier la politique d'entreprise sur les données pour tenir compte d'un nouveau cadre de responsabilisation[12].
- **Créer et tenir à jour un registre des systèmes d'IA** en exploitation et en développement. Ce registre permettra à l'organisation de réagir en cas de problème, par exemple si des données erronées ont été utilisées pour entraîner de multiples algorithmes.
- **Classer les systèmes d'IA par catégorie.** Comme il est indiqué plus haut, les systèmes d'IA peuvent être considérés comme présentant un *risque élevé inacceptable,* un *risque élevé* ou un *risque faible*.
- **Envisager des solutions de rechange aux systèmes d'IA à risque élevé inacceptables.** Rappelons que l'utilisation de systèmes d'IA capables d'influencer ou de manipuler les gens sera déclarée illégale dans l'UE. Par conséquent, on s'attend à ce que les organisations faisant affaire avec le Marché unique européen soient tenues de respecter ces nouvelles restrictions.

10 https://www.iso.org/fr/iso-9001-quality-management.html

11 https://www.iso.org/fr/iso-31000-risk-management.html

12 https://www.cpacanada.ca/fr/voir-demain-initiative/gouvernance-donnees/maitrise-donnees/politique-gestion-donnees-elements

- **Planifier la surveillance humaine** des systèmes d'IA à risque élevé au sein de l'organisation. Comme il est indiqué plus haut, l'organisation doit éviter d'utiliser des systèmes d'IA qui prennent de façon autonome des décisions ayant une incidence sur la santé et la sécurité sans une certaine forme de surveillance humaine. Pour réduire les risques organisationnels, il faut éviter les algorithmes de type « boîte noire », où les décisions ne peuvent être expliquées ou vérifiées par les humains. Il faut également s'assurer que ceux qui sont responsables de la surveillance humaine des systèmes d'IA ont les compétences, ainsi que la formation et l'autorité nécessaires pour s'acquitter de ce rôle.
- **Envisager la création d'un comité ou conseil consultatif sur les systèmes d'IA.** Un tel comité peut être habilité à cerner les risques liés à des résultats non intentionnels, inattendus ou préjudiciables pouvant découler de l'utilisation prévue ou abusive de tous les systèmes d'IA, dont l'IA à faible risque. Il peut également fournir des indications sur l'application de principes pour une IA digne de confiance à la conception et au déploiement des systèmes d'IA[13]. Les normes canadiennes, comme celle du Conseil stratégique des DPI sur la conception éthique et l'utilisation de systèmes de décision automatisés, contiennent de précieuses indications sur la création et le fonctionnement de comités ou conseils consultatifs sur l'IA éthique[14].
- **Envisager l'obtention d'une attestation de tiers concernant les systèmes d'IA à risque élevé** avant leur déploiement. La norme du Conseil stratégique des DPI sur les systèmes de décision automatisés contient des dispositions permettant aux évaluateurs de procéder à des évaluations des incidences éthiques des systèmes d'IA. Grâce à des missions d'attestation ou d'appréciation directe, les organisations peuvent obtenir une assurance sur la conformité, par exemple, d'une allégation de conformité à des normes de gouvernance numérique, dont celle du Conseil stratégique des DPI sur les systèmes de décision automatisés. Selon les Normes canadiennes de missions de certification (p. ex., les NCMC 3000 et 3001) publiées dans le *Manuel de CPA Canada – Certification,* les CPA peuvent réaliser de telles missions de certification et obtenir une assurance limitée ou raisonnable pour les développeurs ou les utilisateurs de systèmes d'IA[15].

13 Par exemple, l'OCDE, par l'entremise de son Conseil sur l'intelligence artificielle, a formulé des recommandations pour une IA digne de confiance en 2019. https://www.oecd.org/fr/numerique/intelligence-artificielle/.

14 Conseil stratégique des DPI. CAN/CIOSC 101:2019, version corrigée de la norme canadienne 2020-09, Conception éthique et utilisation de systèmes de décision automatisés. 23 pages. https://ciostrategycouncil.com/normes/conception-ethique/?lang=fr.

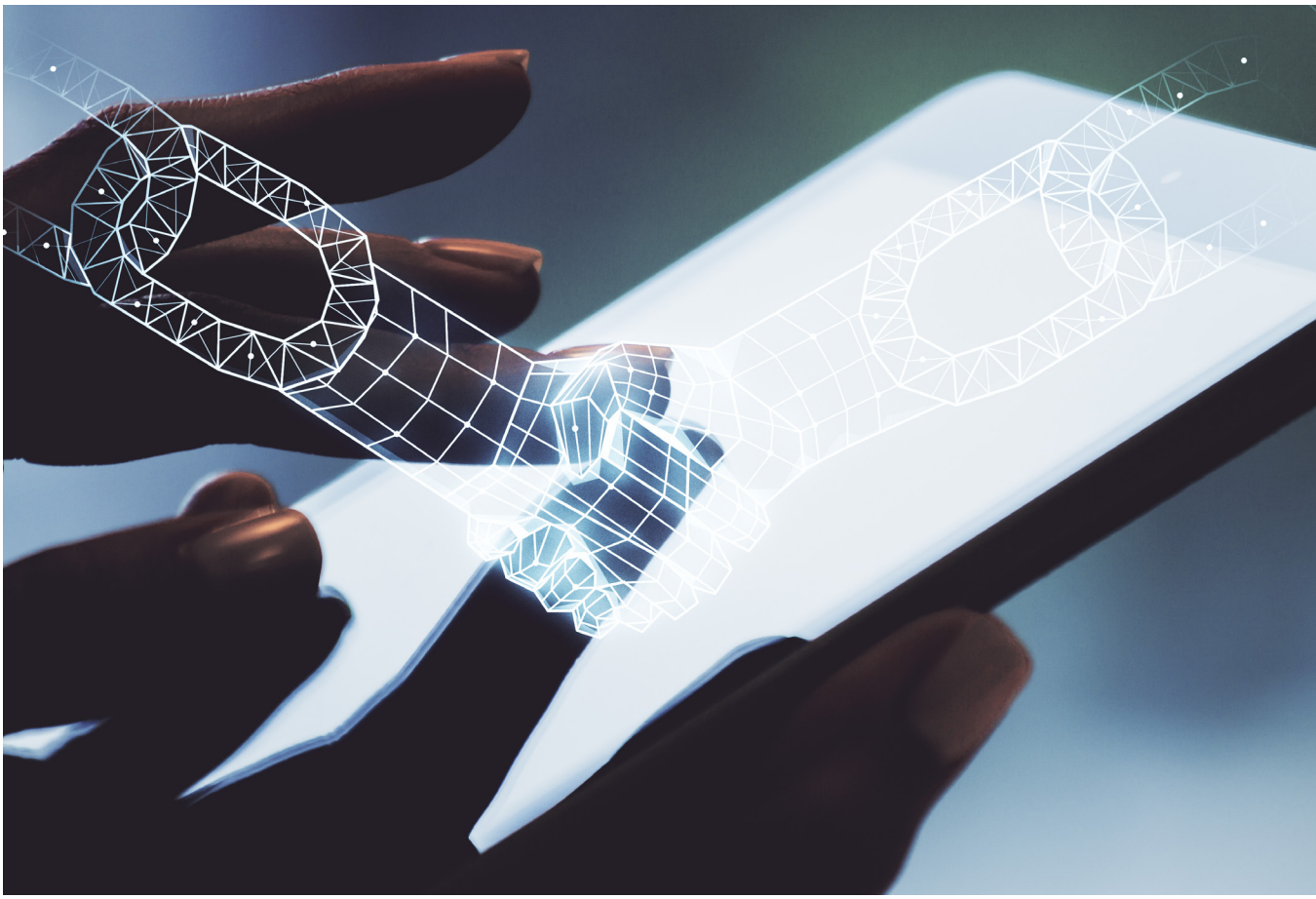
15 CPA Canada. Ce que doivent savoir les auditeurs sur les missions d'attestation et d'appréciation directe. https://www.cpacanada.ca/fr/ressources-en-comptabilite-et-en-affaires/audit-et-certification/normes-autres-que-les-nca-relatives-aux-services-de-certification-et-aux-services-connexes/publications/missions-attestation-appreciation-directe.

- **Mettre l'accent sur la qualité des données.** Si les préjugés découlant d'ensembles de données biaisés peuvent être intégrés dans les algorithmes, ils peuvent aussi s'immiscer dans des ensembles de données incomplets. Les organisations qui déploient des systèmes d'IA doivent s'assurer que les ensembles de données utilisés sont de grande qualité et adaptés aux besoin.
- **Viser la transparence.** L'organisation devrait informer systématiquement les utilisateurs et les clients lorsque ceux-ci interagissent avec l'IA ou des robots, ou lorsque les décisions les concernant sont principalement fondées sur des systèmes d'IA. Il est souhaitable d'établir un mécanisme de recours pour les consommateurs en cas de désaccord quant à une décision générée par un système d'IA[16].

16 CPA Canada. Se doter de données de qualité pour atteindre ses objectifs de transformation numérique. https://www.cpacanada.ca/fr/voir-demain-initiative/gouvernance-donnees/qualite-donnees-vital.

Regard vers l'avenir

Les organisations qui prévoient déployer des systèmes d'IA à risque élevé ont besoin d'un cadre de gestion des risques approprié. Les comptables ont l'habitude de concevoir, de planifier, de mettre en œuvre et de surveiller des programmes de gestion des risques. Ils peuvent jouer un rôle essentiel pour contribuer à combler l'écart entre les données et la confiance. Puisque la gestion des risques encourage la mise en œuvre d'une IA digne de confiance, les comptables peuvent aider leurs organisations à prendre les dispositions voulues pour gérer les risques et faire progresser leur transformation numérique.



CPA COMPTABLES PROFESSIONNELS AGRÉÉS CANADA

277, RUE WELLINGTON OUEST
TORONTO (ONTARIO) M5V 3H2
CANADA
TÉL. : 416 977.3222 TÉLÉC. 416 977.8585

CPACANADA.CA