VOS OBLIGATIONS PROFESSIONNELLES ET DÉONTOLOGIQUES À L'ÈRE DE L'IA

Un guide

CHAMBRE DE L'ASSURANCE DE DOMMAGES

Introduction

L'intelligence artificielle (IA) transforme la manière dont les professionnels en assurance fournissent des conseils et des services à leurs clients. Même si l'adoption de l'IA n'est pas récente, son intégration, son utilisation et son incidence sur les services financiers et d'assurance évoluent rapidement, offrant ainsi de plus en plus de possibilités pour optimiser les processus d'affaires et la prise de décision.

Les certifiés doivent bien comprendre la corrélation entre l'IA générative et leurs obligations professionnelles pour en assurer la conformité.

Le présent guide fournit :

- un survol des trois devoirs déontologiques clés que les certifiés doivent garder à l'esprit lorsqu'ils utilisent l'IA générative (compétence, sécurité et transparence) ;
- des conseils pratiques pour respecter ses obligations déontologiques ;
- des définitions de base ;
- une description des quatre principaux risques connus en lien avec l'utilisation de l'IA.

Les trois grands devoirs déontologiques :

- le devoir de compétence, y compris la compétence technologique ;

- le devoir de confidentialité et de protection des renseignements personnels (sécurité de l'information) ;

- le devoir d'honnêteté et de transparence.

Note : cet outil concerne principalement l'IA générative, mais ne s'y limite pas.

Le Lexique

Intelligence artificielle (IA)

Il existe plusieurs catégories d'IA. Une définition large de l'IA est « la capacité d'une machine à reproduire des comportements ou des activités humaines, tels que le raisonnement, l'apprentissage, la planification et la créativité pour réaliser des activités.[1] »

Système d'intelligence artificielle (SIA)

Système technologique qui, de manière autonome ou partiellement autonome, traite des données au moyen d'algorithmes, de réseaux neuronaux, de l'apprentissage automatique ou d'autres techniques pour générer du contenu, faire des prédictions ou des recommandations ou encore prendre des décisions[2].

IA générative

L'IA générative utilise des données existantes afin de générer « un nouveau contenu similaire aux données sur lesquelles il a été entraîné [3]» (image, texte, audio, code informatique), en réponse à des informations saisies par l'utilisateur, à une question ou à une requête détaillée.

Une des principales caractéristiques de l'IA générative est qu'elle fournit des **réponses aux questions** basées sur des probabilités de réponses, mais sans comprendre le sens du texte généré !

En effet, l'IA peut générer des phrases sémantiquement correctes, mais elle assemble les mots par corrélation statistique, c'est-à-dire les mots les plus susceptibles d'avoir un sens ensemble. Le texte semble avoir un sens, mais l'IA générative ne le comprend pas et le contenu ainsi généré peut, au final, ne rien vouloir dire.

Exemples d'outils d'IA générative :

- les applications populaires, comme ChatGPT ou Copilot, qui reposent sur de grands modèles de langage (GML, ou « LLM » en anglais).
- les outils qui produisent des images à partir de requêtes, tels que DALL-E.

SIA public

Réfère à un SIA développé et déployé pour être accessible à un large public. Toute personne disposant d'une connexion Internet peut s'en servir. Les informations transmises par les requêtes sont traitées sur des serveurs qui ne sont pas contrôlés par l'utilisateur, où les données peuvent être analysées et redistribuées au public. Cette situation soulève des préoccupations concernant la confidentialité et la sécurité des informations.

SIA privé

Réfère à un SIA qui fonctionne dans un environnement fermé et restreint. Un tel système peut provenir d'un tiers ou être développé par l'employeur ou une organisation. Il est intégré aux systèmes informatiques spécifiques d'une organisation. Les informations échangées par les requêtes circulent exclusivement à l'intérieur du réseau de l'organisation, où elles sont stockées et redistribuées selon des critères établis de cette dernière, ce qui réduit les risques.

Requête ou invite (« prompt » en anglais)

Une requête ou invite est une instruction ou une série de directives ou de mots données fournies à un système d'IA, qui utilise ces informations pour générer des réponses ou des créations en texte, image, ou autre forme de média.

1. Inspirée de la définition établie par le Parlement Européen en 2020
2. Tiré du projet de loi C-27, *Loi sur l'intelligence artificielle et les données* (gouvernement fédéral)
3. Prêt pour l'IA, Conseil de l'innovation du Québec, p.4

Les trois grands devoirs déontologiques

1. Devoir de compétence (incluant la compétence technologique)

Les exigences de ce devoir

Les certifiés doivent fournir à leurs clients des services selon la norme d'un représentant compétent et diligent.

Les certifiés doivent **comprendre les technologies** qu'ils utilisent et qui sont mises à leur disposition par leur employeur. Ils doivent pouvoir les employer en tenant compte de la nature et du domaine de leur pratique ainsi que de leurs responsabilités. Les certifiés doivent également comprendre les avantages et les risques inhérents à toute technologie pertinente utilisée dans leur pratique.

Articles pertinents

Loi sur la distribution de produits et services financiers : art.16.

Code de déontologie des représentants en assurance de dommages : art.9 ; art.17, art.37.1, art.37.2.

Code de déontologie des experts en sinistre : art.25, art.26, art.58.1.

L'incidence de l'IA sur ce devoir

Avant d'employer l'IA générative, les certifiés doivent se familiariser avec son fonctionnement, comprendre ses capacités et ses limites, et reconnaitre les risques associés à son utilisation.

Un des pouvoirs uniques de l'IA générative est qu'elle peut créer du nouveau contenu, qu'il s'agisse de mots, d'images ou de sons. Cependant, un outil d'IA générative peut aussi inventer ou incorporer des informations erronées ou trompeuses (appelées communément «hallucinations»), surtout s'il ne dispose pas de données suffisantes pour répondre à une requête. Cela signifie que le contenu généré par l'IA peut ne pas être fiable.

Les certifiés doivent donc prendre des mesures pour vérifier ou assurer l'exactitude des contenus générés afin de respecter ce devoir.

Conseils pratiques

a) **Utilisez votre jugement et votre sens critique.** Reconnaissez que l'IA générative est un outil précieux, mais qu'elle ne remplace pas l'exercice de votre jugement professionnel. Veillez à prendre les mesures nécessaires pour analyser et comprendre de manière critique les résultats de l'IA, et ce, afin de vous assurer de fournir des conseils adéquats et personnalisés en fonction des besoins de vos clients.

b) Assurez-vous de **comprendre les fonctionnalités** de la plateforme utilisée ainsi que ses limites. Vous devez faire preuve de diligence raisonnable lors de l'utilisation du système pour comprendre les résultats générés et vérifier leur pertinence.

c) **Apprenez à rédiger des requêtes efficaces** et adaptées à votre domaine de pratique pour améliorer le contenu généré.

d) **Vérifiez le contenu généré par l'IA** et toute information produite par l'IA générative sur laquelle vous vous appuyez. Le processus de vérification doit être effectué de manière indépendante par un être humain.

e) **Développez, maintenez ou améliorez vos compétences technologiques** en suivant les formations et les outils mis à votre disposition par votre employeur ou des conférences spécialisées. Pratiquez-vous et discutez-en autour de vous !

2. Devoir de confidentialité et de protection des renseignements personnels (sécurité de l'information)

Les exigences de ce devoir

Les certifiés doivent préserver la **confidentialité** de tous les renseignements concernant les affaires et les activités de leurs clients, des assurés ou des sinistrés. Les certifiés ont également l'obligation **de protéger les renseignements personnels** qu'ils recueillent en vertu des lois et règlements applicables.

Articles pertinents

Code de déontologie des représentants en assurance de dommages : art.23 et art.24

Code de déontologie des experts en sinistre : art.22, art.23, art.24

L'incidence de l'IA sur ce devoir

Les certifiés doivent être attentifs aux renseignements qu'ils utilisent dans un système d'IA générative. Selon l'outil d'IA employé, ces informations peuvent se retrouver dans le domaine public, entraînant une violation des obligations de confidentialité et de protection des renseignements personnels.

Par exemple, il ne faut pas téléverser la situation financière ou les données d'un client dans un SIA public pour demander la meilleure assurance ou les meilleures stratégies de gestion du risque d'assurance ! Ces données pourraient être utilisées pour entraîner le SIA ou être rendues accessibles à d'autres.

En revanche, si votre employeur a déployé un SIA privé et fermé intégré au réseau et au système informatiques de l'organisation, et qui s'alimente à même un bassin de données autorisées (p. ex. bibliothèque SharePoint interne de l'entreprise), vous pouvez utiliser le SIA conformément aux directives, et vos obligations de confidentialité seraient respectées.

Conseils pratiques

a) Avant d'employer un SIA, assurez-vous d'en comprendre les risques et vérifiez comment il utilise les données que vous y entrez. Plusieurs SIA utilisent ces données pour former ou améliorer l'outil.

b) La transmission de renseignements personnels doit être limitée aux SIA privés, autorisés et validés par votre employeur.

c) Lorsque le système d'IA générative ne dispose pas de mesures de protection appropriées en matière de confidentialité, de sécurité et de conservation (p. ex. les SIA publics ou qui n'offrent pas les garanties satisfaisantes), **ne saisissez pas** de renseignements personnels, sensibles, confidentiels ou privilégiés.

d) Si la confidentialité ne peut pas être suffisamment protégée en dépersonnalisant les renseignements relatifs au client, expliquez les risques à votre client et obtenez son consentement éclairé avant d'utiliser l'outil.

3. Devoir d'honnêteté et de transparence

Les exigences de ce devoir

Les certifiés ont un devoir d'honnêteté, de franchise et de transparence à l'égard de leurs clients et de leurs mandants. Ce devoir exige que les certifiés informent leurs clients des renseignements dont ils ont connaissance et qui peuvent avoir une incidence sur leurs intérêts.

Articles pertinents

Loi sur la distribution de produits et services financiers : art.16.

Code de déontologie des représentants en assurance de dommages : art.25, art.37.6, art.37.7.

Code de déontologie des experts en sinistre : art.20, art.21, art.27 , art.33, art.58.3 et art.58.5.

L'incidence de l'IA sur ce devoir

Dans un contexte d'intégration ou d'utilisation de l'IA générative, le respect de ce devoir dépendra de plusieurs facteurs, dont :

- La technologie d'IA générative utilisée.
- La manière dont la technologie d'IA générative sera employée et l'objectif poursuivi dans une situation donnée.
- L'incidence possible de la technologie d'IA générative sur les produits ou services offerts.
- Les protocoles et les procédures mis en place par votre organisation et le fournisseur d'IA générative afin de minimiser les risques et d'assurer le respect des règles de conformité.

Lorsque la technologie d'IA générative est pertinente pour les produits et services fournis, mais qu'elle peut nuire aux intérêts des clients ou au règlement de leur dossier de réclamation, ou si les risques associés à la technologie d'IA générative sont préoccupants, les certifiés devraient informer les clients qu'ils utilisent cette technologie.

Dans ces situations, les certifiés devraient être prêts à expliquer aux clients comment ils utilisent la technologie dans leur dossier, les risques qui y sont associés et les mesures prises pour les atténuer.

Conseils pratiques

a) Analysez les facteurs et les circonstances de l'utilisation de l'IA générative et évaluez si la divulgation de cette utilisation est nécessaire pour fournir vos services.

b) Si la divulgation est indiquée, soyez prêt à fournir des renseignements aux clients sur les avantages et les risques inhérents à la technologie d'IA générative employée.

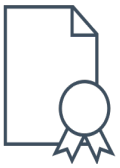
c) Si possible, utilisez des marques, des filigranes (tatouage numérique) ou une mention pour identifier le contenu (ou une partie du contenu) généré par l'IA.

d) Si l'entreprise utilise des robots conversationnels d'IA générative, les consommateurs doivent pouvoir s'attendre à ce que l'entreprise fasse preuve de transparence à cet égard et que des mesures de protection appropriées soient prises afin d'éviter les malentendus avec les clients et la transmission de faux renseignements.

Les principaux risques de l'IA en lien avec vos obligations déontologiques

Comme pour toute avancée technologique, l'IA vient avec plusieurs avantages, mais aussi avec nombre d'enjeux qu'il faut garder à l'esprit. Voici les enjeux plus fréquemment mentionnés en lien avec les obligations déontologiques des professionnels :

1. Exactitude, véracité et fiabilité :



Hallucinations, informations inventées ou inexactes : dans le domaine de l'IA, une hallucination est une réponse fausse, inventée, incohérente ou inexacte, mais présentée comme valide.

Dans la pratique d'un certifié, cela pourrait être une explication ou un résumé des garanties erronés ou encore une évaluation inexacte des biens à assurer ou des pertes assurables.

Hypertrucage (« deepfake ») : L'hypertrucage consiste en la modification ou la manipulation d'images ou d'enregistrements pour faire croire que quelqu'un a fait ou dit quelque chose qui n'a pas été fait ou dit en réalité. La technologie existe depuis longtemps (p. ex. Photoshop, courriels ou messages frauduleux qui semblent provenir d'une source fiable), mais les avancées de l'IA permettent désormais d'obtenir des résultats plus réalistes et convaincants. Outre les tentatives de fraude à l'égard des particuliers et des entreprises (p. ex. pour soutirer de l'argent), l'hypertrucage peut porter atteinte à la réputation d'une personne ou d'une entreprise si de fausses images ou vidéos sont créées et rendues publiques.

Dans la pratique d'un certifié, un hypertrucage (p. ex. l'imitation de la voix d'un client ou d'un dirigeant) pourrait être utilisé pour tenter de frauder votre entreprise ou celle d'un client, modifier les protections d'assurance ou soutirer des renseignements personnels à des fins malveillantes.

2. Atteintes à la vie privée et informations confidentielles :

Par définition, les SIA utilisent les informations et données fournies dans une requête (invite, ou « prompt ») pour générer une réponse, information ou calcul. Ces données, si elles sont personnelles ou confidentielles, peuvent être gérées ou stockées de manière non sécuritaire, ou utilisées pour entraîner le modèle, sans consentement approprié.

Par exemple, si un certifié écrit une requête destinée à un SIA public en y intégrant des informations à propos d'un client (adresse, cote de crédit, etc.), cela porte atteinte à la vie privée de ce dernier et ne respecte pas l'obligation de protéger ses informations personnelles et confidentielles.

3. Biais discriminatoires :

Les biais existent en dehors de l'IA et peuvent mèner à des décisions humaines parfois incorrectes, ou subjectives et discriminatoires. Ils peuvent donc être reproduits par des SIA, mais aussi être amplifiés de façon significative, car intégrés dans les algorithmes employés par les SIA (par exemple, en utilisant des données biaisées, incomplètes ou insuffisantes statistiquement).

Par exemple, un expert en sinistre qui utilise un SIA pour effectuer une analyse de la recevabilité des réclamations. Si les données utilisées pour entraîner le modèle sont elles-mêmes biaisées, le SIA pourrait refuser une plus grande proportion de réclamations ou offrir des montants moindres sur la base de motifs de discrimination interdits.

4. Droits d'auteur et propriété intellectuelle :

Les modèles d'IA générative sont entraînés à partir de grandes quantités de données, d'images, de textes et autres obtenus de sources différentes, souvent à même des bases de données publiques. Cependant, ces contenus pouvant être sujets à des droits d'auteur, l'utilisation non autorisée et non déclarée de leur contenu pour former des SIA génératives est susceptible de violer les droits applicables.

Par exemple, un certifié qui utilise une référence (texte, son ou image) trouvée à l'aide d'un SIA sans autorisation de l'auteur ou sans citer la source pour la partager sur son réseau social professionnel.

Conclusion
L’indépendance professionnelle et l’IA

L’indépendance professionnelle est le fait d'exercer sa profession avec objectivité et de faire abstraction de toute intervention d’un tiers qui pourrait influer sur l’exécution de ses obligations professionnelles. Il faut respecter l’esprit des codes de déontologie pour éviter de causer préjudice au client. En ce sens, **l’indépendance professionnelle** peut être considérée comme une obligation qui chapeaute les autres devoirs déontologiques.

En assurance de dommages, cette notion signifie que le certifié doit toujours exercer son jugement professionnel dans l’intérêt du client. Pour en savoir plus, veuillez lire l’article « Les obligations déontologiques prévalent. »

De la même façon, l’utilisation de l’IA continuera à se développer et promet des améliorations substantielles dans de nombreux domaines, dont celui de l’assurance de dommages. Cependant, les certifiés doivent faire preuve de jugement et maintenir un esprit critique à l’égard de l’utilisation de l’IA dans leur pratique : un SIA est un outil pour vous soutenir dans votre travail, sans remplacer votre expertise et votre jugement.