

# Déchiffrer demain : l'abécédaire BLG sur la gouvernance de l'IA



## Qu'est-ce qu'un cadre de gouvernance de l'IA et pourquoi votre organisation en a-t-elle besoin ?

Les cadres de gouvernance de l'IA sont essentiels pour les organisations qui cherchent à exploiter l'incroyable potentiel de l'IA aujourd'hui tout en assurant leur conformité avec la réglementation actuelle et future. Les divers risques liés à l'utilisation de l'IA, tels que les résultats biaisés et l'atteinte à la confidentialité des données, accentuent la nécessité de se pencher sur les enjeux juridiques, commerciaux et réputationnels liés à l'utilisation de cette technologie, en particulier dans le sillage des récents développements réglementaires en Europe et au Canada. Les organisations naviguent dans ce contexte en pleine évolution en intégrant dans leur gouvernance les obligations existantes et les meilleures pratiques de cadres non contraignants tout en anticipant les développements juridiques dans ce domaine. Un cadre de gouvernance de l'IA est un atout précieux qui permet aux organisations d'assurer la pérennité de leurs opérations, de se préparer aux changements réglementaires et de renforcer leur résilience dans leur déploiement de l'IA.

## Quels sont les éléments clés d'un programme de gouvernance de l'IA ?



### 1) Gouvernance

**Principes directeurs.** Une équipe multidisciplinaire composée des principaux responsables de la gestion des risques, du service juridique et du développement des produits de l'organisation devrait établir des principes d'IA alignés sur les valeurs fondamentales de l'organisation, sur la réglementation à venir en matière d'IA et sur les normes pertinentes en matière de gouvernance de l'IA.

**Structure organisationnelle.** Les organisations devraient désigner une personne et/ou un comité chargé de faire

#### Responsabilisation

respecter leurs principes directeurs en matière d'IA. Ce rôle, qui s'apparente à celui d'un responsable de la protection de la vie privée et de son équipe dans le domaine de la protection de la vie privée, devrait inclure des personnes spécialisées dans la gestion des risques et de l'information, ainsi que dans les questions juridiques. Les titres suivants peuvent être utilisés pour désigner les rôles au sein de cette structure interne : responsable de l'IA, conseiller en gouvernance de l'IA et comité d'éthique de l'IA.



### 2) Cartographie

Les organisations doivent identifier chaque système d'IA qu'elles utilisent et ses objectifs. Au cours de ce processus, les organisations doivent donner la priorité aux systèmes d'IA ayant un impact potentiellement élevé sur les personnes, et documenter si chaque système d'IA identifié implique le traitement de renseignements personnels et la juridiction dans laquelle résident les personnes concernées par son utilisation.

#### Responsabilisation et Sûreté



### 3) Classification en fonction du risque

Les organisations devraient évaluer les risques liés aux systèmes d'IA qu'elles utilisent, déterminer l'ampleur de ces risques et les classer de manière appropriée. Ceci implique d'examiner attentivement les indicateurs d'atteinte potentielle à la santé et à la sécurité des individus, ainsi que d'évaluer le risque d'incidences négatives sur les droits fondamentaux. En outre, les organisations doivent vérifier si les systèmes d'IA sont déployés dans des secteurs reconnus pour leur impact significatif sur la vie des individus, tels que l'accès aux services, l'application de la loi et l'éducation.

#### Confidentialité et Sécurité et Sûreté

#### 4) Évaluation et mitigation des risques

**Évaluation des systèmes d'IA.** Les organisations devraient sélectionner des méthodes et des paramètres pour évaluer les systèmes d'IA afin d'identifier les risques spécifiques liés à leur utilisation. Par exemple, les organisations peuvent évaluer si un système d'IA est susceptible de produire des résultats biaisés au moyen d'audits d'équité et elles peuvent mesurer la sécurité des systèmes d'IA au moyen de tests de fiabilité et d'indicateurs liés aux taux de défaillance.

**Mitigation des risques.** Les organisations devraient mettre en œuvre des mesures de mitigation en réponse aux risques identifiés et documenter les risques résiduels. Chaque organisation doit adapter ses mesures de mitigation en fonction de sa tolérance au risque, de ses principes directeurs en matière d'IA et de ses objectifs commerciaux.

#### 5) Élaborer des politiques et des procédures organisationnelles

Chacun des principes directeurs définis par l'organisation doit être mis en œuvre par l'élaboration de politiques, de procédures et d'outils internes et externes pertinents, tels qu'une politique régissant l'utilisation de l'IA générative, un modèle d'évaluation d'impact algorithmique et un avis public en langage clair concernant l'usage de de l'IA.

#### 6) Surveillance

Les organisations doivent mettre en place un processus de vérification continue de l'évaluation des risques posés par leurs systèmes d'IA, ainsi qu'une révision régulière des politiques et procédures élaborées. La mise en œuvre de ces stratégies de surveillance est essentielle pour garantir que le cadre de gouvernance de l'IA puisse s'adapter à l'évolution des risques, des technologies et des pratiques du secteur.

Avec l'encadrement juridique spécifique à l'IA qui se profile à l'horizon, votre organisation peut prendre une longueur d'avance en implantant des mesures proactives garantissant ainsi des opérations ininterrompues tout en libérant le plein potentiel de l'IA.

Pour plus d'information veuillez contacter :



**Frédéric Wilson**  
Avocat-conseil  
514.954.2509  
FWilson@blg.com



**Simon Du Perron**  
Avocat  
514.954.2542  
SDuperron@blg.com