OSLER

PERSPECTIVES JURIDIQUES OSLER 2023

Gouvernance de l'intelligence artificielle : composer avec ce que l'avenir nous réserve

11 DÉCEMBRE 2023 10 MIN DE LECTURE

Expertises Connexes

- Intelligence artificielle
- Technologie

Auteurs(trice): Simon Hodgett, Sam Ip

Il va sans dire qu'au cours de la dernière année, un changement remarquable et radical s'est opéré dans le secteur canadien de l'intelligence artificielle (IA) avec l'émergence des technologies d'IA générative et leur adoption fulgurante. Cette adoption rapide a été accompagnée d'une vague de mesures législatives et réglementaires qui pourraient avoir une incidence considérable sur l'utilisation et l'adoption de l'IA et des technologies connexes.

Les technologies révolutionnaires et les changements réglementaires présentent des défis pour les entreprises. L'IA leur procure des avantages, mais soulève aussi de nouveaux risques. Les équipes de direction doivent aborder la question de la responsabilisation en matière d'utilisation de l'IA, en mettant en œuvre des politiques et des procédures appropriées, entre autres mesures. Il est essentiel de comprendre le risque lié à la propriété intellectuelle et la protection de celle-ci. Parallèlement, les organisations doivent prendre des mesures concrètes pour gérer les risques associés à l'IA, au moyen entre autres de solides programmes de conformité, de la transparence quant à l'utilisation de l'IA et de l'adoption de normes d'éthique et de codes de conduite.

En 2024 et au-delà, les entreprises devront évaluer de façon proactive les avantages de l'IA, prendre des mesures pour atténuer les risques et composer avec un cadre réglementaire et éthique de plus en plus complexe.

Multiplication des changements réglementaires en matière d'IA

En très peu de temps, un certain nombre de modifications législatives et de nouvelles directives ont été proposées; elles pourraient avoir une incidence profonde sur l'adoption et l'utilisation des technologies d'IA.

Le gouvernement fédéral canadien a déposé la *Loi sur l'intelligence artificielle et les données* (LIAD), qui constitue un élément clé de la Charte canadienne du numérique proposée. La LIAD a passé les étapes de la première et de la deuxième lecture et est actuellement à l'étude devant le Comité permanent de l'industrie et de la technologie.

Par ailleurs, le Conseil de gouvernance numérique a proposé des normes pour aider les

innovateurs canadiens en matière de technologie financière à faire face aux risques associés aux solutions d'IA et d'apprentissage automatique utilisées par les institutions financières. De plus, le Bureau du surintendant des institutions financières et le Global Risk Institute ont publié un rapport conjoint fournissant des orientations sur l'IA pour les institutions financières.

Enfin, le gouvernement fédéral canadien a également collaboré avec diverses entreprises pour préparer un Code de conduite volontaire visant un développement et une gestion responsables des systèmes d'IA générative avancés. Il ne fait aucun doute que d'autres changements sont à venir.

Grandes questions entourant la gouvernance de l'IA

L'adoption et l'utilisation des technologies d'IA exigent une stratégie globale qui encadre l'ensemble de l'organisation. Comme point de départ, les organisations doivent établir un cadre de gestion des risques proportionnel à l'ampleur et à l'incidence de leurs activités liées à l'IA, cadre pouvant être mis en œuvre de façon pratique.

La première étape consiste à évaluer comment l'organisation compte faire usage de l'IA et à établir s'il s'agit d'une organisation qui conçoit, qui déploie ou qui utilise des solutions d'IA. En effet, un utilisateur n'aura pas les mêmes préoccupations et ne sera pas exposé aux mêmes risques qu'un concepteur. Dans la mise en place d'un cadre de gestion des risques, une organisation doit définir sa stratégie et ses objectifs globaux en matière d'IA en s'appuyant sur son degré de tolérance au risque. Il est ensuite préférable de déléguer à un ou plusieurs responsables la mise en œuvre du cadre et la responsabilité globale de l'adoption de l'IA de façon sécuritaire et fiable.

Enfin, il est essentiel d'établir des politiques et des protocoles en ce qui concerne l'utilisation de l'IA par l'organisation. Ce processus devrait déterminer comment la sécurité, l'équité et la transparence seront prises en compte. Ces politiques et ces protocoles devraient définir les cas dans lesquels l'utilisation de l'IA est autorisée. La surveillance par un humain est également essentielle, tout comme des lignes directrices quant aux modalités d'évaluation du rendement du système d'IA. Il est également important de déterminer comment les problèmes seront signalés, transmis à un échelon supérieur et résolus au sein de l'organisation.

Il existe un vaste éventail de ressources qui fournissent des orientations quant à l'adoption de cadres de gestion des risques liés à l'IA. Par exemple, le AI Risk Management Framework (cadre de gestion des risques liés à l'IA) du NIST (National Institute of Standards and Technology) énonce des principes que les organisations peuvent intégrer à leurs stratégies de gouvernance existantes afin de gérer les risques propres à l'IA.

En établissant un nouveau cadre, les organisations doivent évaluer leurs politiques existantes et déterminer s'il est nécessaire d'en adopter de nouvelles, propres à l'IA, ou si les politiques en place doivent être adaptées. Par exemple, il pourrait s'avérer nécessaire d'apporter des précisions aux politiques existantes relatives à la confidentialité dans un contexte d'utilisation de l'IA. De telles dispositions devraient entre autres mettre l'accent sur la nécessité de faire preuve de prudence en ce qui concerne la soumission de renseignements sensibles, confidentiels ou exclusifs à des services d'IA générative. Une telle prudence est essentielle en ce qui a trait non seulement à l'utilisation de l'IA générative, mais aussi aux données de formation servant à concevoir et à améliorer les modèles d'IA qui sous-tendent ces services.

Des politiques particulières peuvent être nécessaires pour les utilisations techniques de l'IA, y

compris des règles de base relatives au recours à l'IA générative comme outil d'aide au codage. Ces politiques doivent définir les activités de développement à faible risque, comme la conception d'un code pour les besoins internes de l'organisation. Elles devraient également veiller à ce que des mesures de protection appropriées soient en place pour les utilisations assorties d'un risque élevé, comme l'examen par un humain du code généré.

En plus de politiques et de procédures, les organisations devraient élaborer des stratégies de communication et de formation en lien avec l'IA. Il importe de concevoir des communications internes et des formations sur l'utilisation appropriée des outils d'IA à l'appui de protocoles de conformité adaptés au cadre de gestion des risques. Les organisations doivent également être en mesure d'expliquer aux parties externes les mesures prises pour réduire les biais et les enjeux d'équité potentiels liés aux systèmes d'IA qu'elles conçoivent ou utilisent.

Compte tenu de la complexité de l'environnement et de son évolution rapide, il est nécessaire de tenir compte de questions juridiques et éthiques aux étapes appropriées du cycle de développement d'une solution d'IA. Cette approche est particulièrement utile au début du processus de développement, lorsque la mise en place de mesures visant à atténuer les risques peut s'avérer plus facile et plus économique. Les principes fondamentaux de l'IA responsable, comme la conception fondée sur des questions éthiques, peuvent être intégrés dès le départ. Compte tenu de l'importance des questions liées à la protection appropriée de la vie privée, des experts en la matière, en particulier ceux qui maîtrisent les cadres de conception fondée sur la protection de la vie privée, devraient être sollicités pour conseiller les équipes de développement affectées à l'IA.

La plupart des organisations technologiques ont mis en œuvre des mesures de protection de la propriété intellectuelle qui s'appliquent aux logiciels et aux codes sources connexes. Il est cependant possible que les cadres existants ne protègent pas adéquatement les modèles d'IA, leurs attributs et leur architecture. Les organisations doivent examiner attentivement comment protéger ces modèles et comment préserver adéquatement la propriété des améliorations à mesure qu'évoluent les solutions. Dans le cadre des relations avec des tiers et des ententes commerciales, un des éléments importants de la protection de la propriété intellectuelle consiste à assurer l'intégration de modalités qui définissent les paramètres propres à l'IA (comme les modèles, les pondérations et les biais, et les architectures des modèles) et à délimiter clairement la propriété de ces éléments. Les définitions générales relatives à la propriété intellectuelle et aux données qui figurent dans les contrats ne précisent pas toujours qui a la propriété de ces éléments.

De plus, les contrats commerciaux relatifs à la fourniture de solutions d'IA constituent un moyen efficace de veiller à ce que l'entente en question cadre avec les politiques d'IA et les exigences législatives de l'organisation. La répartition des risques dans les contrats commerciaux peut également refléter le degré de tolérance au risque de l'organisation à l'égard des applications d'IA, ainsi que ses attentes quant à des cas d'utilisation précis. Les contrats peuvent être utilisés pour garantir que le fournisseur d'IA s'engage à respecter l'évolution des normes, à proposer une solution explicable et à la mettre à l'essai pour déceler tout biais.

Les données alimentent l'IA. Un cadre exhaustif de gestion des risques doit aborder la collecte, l'utilisation et la communication des données conformément aux règlements applicables, y compris les lois sur la protection de la vie privée. Les politiques relatives au transfert et à la communication de données doivent être conçues pour veiller à ce que ces activités ne soient réalisées qu'après avoir obtenu les consentements nécessaires et les autorisations contractuelles. Les protocoles doivent également assurer l'évaluation préalable de la disponibilité, de la quantité et de la pertinence des ensembles de données utilisés pour soutenir des solutions qui donnent des résultats exploitables et conformes à la loi. Par exemple, les entrées de données doivent constituer un échantillon suffisamment grand. Des mesures doivent également être en place pour réduire les biais au minimum et gérer les

biais indésirables et ainsi garantir des résultats justes et équitables.

Compte tenu du grand nombre d'aspects de l'IA en cours d'évolution, sans parler de la multitude de normes, de lignes directrices et de nouveaux règlements, les organisations se retrouvent manifestement débordées. Heureusement, des solutions visant à assurer le suivi des exigences relatives à l'IA sont en cours d'élaboration. Les organisations doivent demeurer à l'affût de ces solutions à mesure qu'elles font leur arrivée sur le marché et qu'elles s'inscrivent en tant que pratiques courantes. Ces outils peuvent aider à transformer les exigences des politiques globales en mesures de contrôle exploitables, en évaluations des impacts sur les systèmes, en mesures de protection des systèmes et en relevés des modèles.

Perspectives

La rapidité de l'innovation touchant les applications d'IA est stupéfiante et la complexité des questions relatives aux politiques, à l'éthique et aux lois est appelée à augmenter de façon exponentielle au cours des semaines, des mois et des années à venir. Les organisations doivent se préparer en vue de cette transformation technologique rapide et prendre des mesures proactives pour veiller à ce que des politiques et des protocoles appropriés soient en place, conformément aux exigences réglementaires et au degré de tolérance au risque de l'entreprise.