La définition juridique de l'intelligence artificielle évolue : différents pays, différentes approches

10 mars 2020

Auteur

Eric Lavallée

Associé, Agent de marques de commerce Associé, et Avocat

Alors que notre société commence à apprivoiser l'intelligence artificielle, les législateurs de plusieurs territoires sont confrontés aux inquiétudes de la population ainsi qu'à la volonté de tirer profit de ces technologies pour le bien public. La réflexion est bien entamée dans plusieurs pays, mais avec des résultats variables.

Le Commissariat à la protection de la vie privée du Canada consulte présentement des experts afin de formuler des recommandations au Parlement. On vise par cette démarche à déterminer si des règles particulières relatives à la vie privée doivent s'appliquer lorsque l'intelligence artificielle est en cause. Notamment, le Canada devrait-il adopter un régime s'approchant du régime européen (RGPD)? De plus, on y soulève la possibilité d'adopter des mesures similaires à ce que propose le projet d'*Algorithmic Accountability Act* de 2019 présenté au Congrès américain, qui donnerait à la Federal Trade Commission des États-Unis le pouvoir de contraindre les entreprises à évaluer les risques liés à la discrimination et à la sécurité des données des systèmes d'intelligence artificielle. La Commissions d'accès à l'information du Québec procède actuellement à des consultations sur le même sujet.

L'approche américaine semble aussi vouloir favoriser le positionnement commercial de ce pays dans le domaine de l'intelligence artificielle. Le National Institute of Standards and Technology (NIST) a publié le 9 août 2019 une ébauche de plan d'action gouvernemental, en réponse à un ordre exécutif du président américain. Cette ébauche, *U.S. LEADERSHIP IN AI : A Plan for Federal Engagement in Developing Technical Standards and Related Tools*[1], préconise notamment la mise au point de nouvelles technologies robustes pour augmenter la fiabilité des solutions incorporant l'intelligence artificielle, ainsi que le développement de normes standardisées pour ces technologies.

En parallèle, le service de recherche du Congrès a publié le 21 novembre 2019 une mise à jour de son mémoire intitulé *Artificial Intelligence and National Security*[2]. Ce document présente une réflexion sur les applications militaires de l'intelligence artificielle, notamment sur le fait que divers dispositifs de combat puissent mener des attaques létales de manière autonome. On y réfléchit aussi sur les moyens de contrer les « deep fake », notamment par la mise au point de technologies

pour débusquer ce qui pourrait devenir un moyen de désinformation. On mise donc sur le progrès technologique pour déjouer la technologie utilisée à mauvais escient.

En Europe, à la suite de consultations achevées en mai 2019, un groupe d'experts sur la responsabilité et les nouvelles technologies a produit un rapport à l'intention de la Commission Européenne, intitulé *Liability for Artificial Intelligence*[3], qui présente une réflexion sur les régimes de responsabilité applicables à de telles technologies. Le groupe souligne que sauf pour les questions de renseignements personnels (RGPD) et celles concernant les véhicules automobiles, les régimes de responsabilité des états membres ne sont pas harmonisés en Europe. Le groupe d'experts recommande notamment d'harmoniser les régimes de responsabilité. Selon eux, des risques comparables devraient être encadrés par des régimes de responsabilité similaires[4].

Plus tôt, en janvier 2019, le Comité consultatif de la Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel du Conseil de l'Europe, avait émis des *Lignes directrices sur l'intelligence artificielle et la protection des données*[5], offrant notamment des recommandations aux législateurs, mais aussi aux développeurs, fabricants et prestataires de services qui utilisent de telles technologies afin de se conformer aux conventions en matière de droits de l'homme.

Mais à travers ces différences d'approche, une question fondamentale subsiste : si des règles particulières doivent être adoptées, à quelles technologies doit-on les appliquer? Il s'agit là d'une des questions fondamentales posée par le Commissariat à la protection de la vie privée au Canada.

En d'autres termes, qu'est-ce que l'intelligence artificielle? L'expression n'est pas clairement définie d'un point de vue technologique. Elle représente un vaste ensemble de technologies ayant des caractéristiques et des modes de fonctionnement diversifiés.

C'est donc la première question à laquelle devront s'attaquer les législateurs s'ils souhaitent mettre au point un cadre juridique spécifique aux technologies d'intelligence artificielle.

Le document du groupe d'experts européen cité ci-dessus nous donne quelques pistes de réflexion qui nous semblent pertinentes. Selon eux, on doit prendre en considération les facteurs suivants pour la qualification de la technologie :

> sa complexité;
> son aspect opaque;
> son ouverture à l'interaction avec d'autres solutions technologiques;
> son degré d'autonomie;
> la prévisibilité des résultats;
> le fait qu'elle se fonde sur des quantités importantes de données, et
> sa vulnérabilité aux attaques et risques informatiques.

Ces facteurs contribuent à cerner les risques inhérents aux différentes technologies, au cas par cas.

De manière générale, il nous semble préférable de ne pas adopter un ensemble de critères rigides devant s'appliquer à toutes les technologies. Nous suggérons plutôt de cerner les objectifs législatifs en fonction de caractéristiques pouvant se retrouver dans plusieurs technologies. On peut par exemple penser qu'une technologie d'apprentissage profond peut parfois utiliser des renseignements personnels, et parfois ne requérir aucun tel renseignement ou très peu. Une telle technologie peut dans certains cas prendre des décisions de manière autonome, alors que parfois, elle ne sera qu'un soutien à la décision. Enfin, si certaines technologies permettent une certaine transparence, d'autres demeureront plus opaques, et ce parfois en raison des contraintes de nature technologiques ou commerciales.

Pour les développeurs, il importe également de qualifier correctement la solution envisagée afin de mesurer les risques afférents à son exploitation commerciale. Plus précisément, il peut être

important de réfléchir avec des juristes de différents horizons pour s'assurer que la solution proposée n'est pas complètement incompatible avec les lois présentement applicables dans les différents territoires où elles seront déployées, mais aussi avec les lois qui pourraient être adoptées à court terme dans ces territoires.

---

1. https://www.nist.gov/system/files/documents/2019/08/10/ai_standards_fedengagement_plan_9aug2019.pdf
2. https://fas.org/sgp/crs/natsec/R45178.pdf
3. https://ec.europa.eu/transparency/regexpert/index.cfm?do=groupDetail.groupMeetingDoc&docid=36608
4. Idem, p. 36.
5. https://rm.coe.int/lignes-directrices-sur-l-intelligence-artificielle-et-la-protection-de/168091ff40