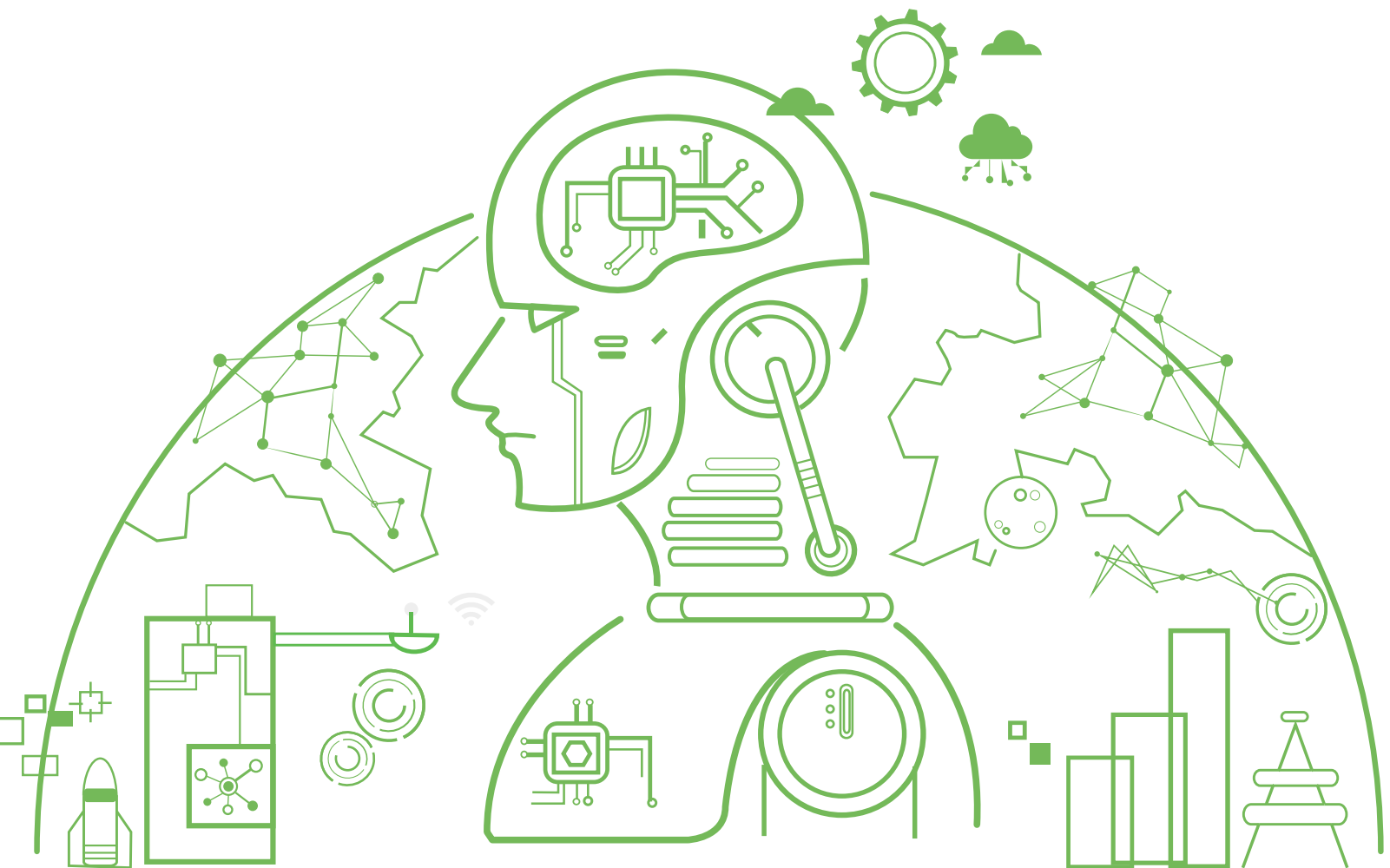


De la propriété intellectuelle à la cybersécurité :

*les enjeux juridiques de
l'intelligence artificielle.*



Lavery Avocats a mis sur pied le Laboratoire juridique Lavery sur l'intelligence artificielle (L³IA) qui analyse et suit les développements récents et anticipés dans le domaine de l'intelligence artificielle d'un point de vue juridique. Notre Laboratoire s'intéresse à tous les projets relatifs à l'intelligence

artificielle (IA) et à leurs particularités juridiques, notamment quant aux diverses branches et applications de l'intelligence artificielle qui feront rapidement leur apparition dans toutes les entreprises et les industries.

Index

- 04 Intelligence artificielle : la délicate interaction entre les défis juridiques et technologiques
- 22 Intelligence artificielle : les obligations contractuelles au-delà de l'expression à la mode
- 26 Intelligence artificielle, implantation et ressources humaines
- 34 La propriété intellectuelle de l'intelligence artificielle
- 42 Lorsque l'intelligence artificielle est discriminatoire
- 50 Intelligence artificielle et chaînes de blocs : vulnérables aux cyberattaques
- 58 La conduite des voitures autonomes au Québec : plusieurs questions demeurent

Intelligence artificielle : la délicate interaction entre les défis juridiques et technologiques

Par : **Jean-Sébastien Desroches**
et **Shan Jiang**

Existe-t-il un plus grand défi que celui d'écrire un article juridique sur une technologie émergente qui n'existe pas encore sous sa forme absolue ?

L'intelligence artificielle, par l'intermédiaire d'un large éventail de branches et d'applications, aura des incidences sur divers domaines de la pratique du droit, dont l'éthique et l'intégrité en

entreprise, la gouvernance, la distribution des produits et services financiers, la propriété intellectuelle, la protection de la vie privée et des informations, le droit du travail et de l'emploi, la responsabilité civile et contractuelle, de même que sur un nombre important d'autres disciplines du droit.

Qu'est-ce que l'intelligence artificielle ?

L'intelligence artificielle est (traduction libre) « la science combinée à l'ingénierie dans le cadre de la fabrication de machines intelligentes, particulièrement des logiciels intelligents »¹. Essentiellement, le but de l'intelligence artificielle est de permettre aux machines d'imiter les fonctions « cognitives » de l'être humain, telles que l'apprentissage et la résolution de problèmes, de façon à ce qu'elles puissent exécuter des tâches qui sont normalement effectuées par des êtres humains. De façon pratique, les

fonctionnalités de l'intelligence artificielle dépendent souvent de l'accès à des quantités colossales de données (« mégadonnées ») par l'intermédiaire de certains algorithmes et de la capacité de traitement de celles-ci.

Tel qu'il est souligné dans un rapport publié par McKinsey & Company en 2015 sur les technologies révolutionnaires (traduction libre) « [d]es technologies importantes peuvent être mises au point dans n'importe quel secteur ou provenir

de n'importe quelle discipline scientifique, mais elles partagent quatre caractéristiques : la grande rapidité des changements technologiques, un potentiel de vaste portée des impacts, des enjeux financiers importants et un fort potentiel pour une incidence économique perturbatrice »².

En marge du débat intéressant concernant l'incidence possible de l'intelligence artificielle sur l'humanité³, son perfectionnement a été mis sur la voie rapide dans les dernières années et nous avons assisté à plusieurs percées importantes. En mars 2016, le logiciel Alpha-Go de Google a battu Lee Sedol, champion mondial de Go, par une marque de 4 à 1 à cet ancien jeu de société chinois. Ces percées ont ravivé l'intérêt des communautés d'affaires pour l'intelligence

artificielle. Des géants de la technologie tels que Google et Microsoft, pour n'en nommer que quelques-uns, ont accéléré leurs investissements dans la recherche et l'amélioration de systèmes reposant en partie sur l'intelligence artificielle.

Le présent article aborde certaines facettes de l'intelligence artificielle d'un point de vue juridique et traite de certains domaines du droit qui devront s'adapter aux défis complexes résultant des nouveautés actuelles et à venir en matière d'intelligence artificielle.

¹ John McCarthy, What is artificial intelligence?, Stanford University: <http://www-formal.stanford.edu/jmc/whatisai/>.

² Disruptive technologies: Advances that will transform life, business, and the global economy, McKinsey Global Institute, May 2013.

³ Alex Hern, Stephen Hawking: AI will be "either best or worst thing" for humanity, theguardian: <https://www.theguardian.com/science/2016/oct/19/stephen-hawking-ai-best-or-worst-thing-for-humanity-cambridge>.



Défis juridiques certains

Les incidences possibles de l'intelligence artificielle ont été maintes fois comparées à celles de la révolution industrielle, c'est-à-dire une forme de transition vers de nouveaux processus de fabrication utilisant de nouveaux systèmes, de même que l'usage accru d'applications et des machines innovantes.

Domaine de la santé

L'intelligence artificielle est certes promise à un bel avenir dans le secteur des soins de santé. Les applications d'intelligence artificielle capables d'analyser des tonnes de données dans un délai record peuvent faire de ces applications des outils puissants permettant de prédire, par exemple, le succès de certains médicaments et d'aider les patients à trouver la bonne dose de médicaments compte tenu de multiples facteurs. Récemment, la société IBM a confirmé que son programme IBM Watson Health « est capable de comprendre et d'extraire de l'information clé en consultant des millions de pages

de littérature scientifique médicale pour ensuite visualiser des relations entre les médicaments et d'autres maladies potentielles »⁴. D'autres applications de l'intelligence artificielle peuvent également aider à vérifier si un patient a pris ses comprimés au moyen d'un téléphone intelligent qui capte et analyse les signes ou les effets confirmant que le médicament a bel et bien été ingéré.

En plus des préoccupations visant la protection de la vie privée et des informations personnelles, qui constituera inévitablement un enjeu complexe, les plateformes

d'intelligence artificielle dans le domaine de la santé pourraient soulever des défis juridiques importants, notamment au niveau de la responsabilité civile et contractuelle. Si un médecin ou un patient suit les recommandations effectuées par un système d'intelligence artificielle et que ces recommandations s'avèrent erronées, qui en sera tenu responsable en dernier ressort ?

L'intelligence artificielle soulève donc des questions juridiques légitimes et complexes dans le domaine de la santé, combinées à des préoccupations de nature technologique touchant la fiabilité des logiciels, plateformes et autres programmes d'intelligence artificielle ainsi que la façon dont les professionnels, employés et autres intervenants utiliseront ces applications dans le cadre de leurs tâches et responsabilités quotidiennes.



⁴ Engene Borukhovich, How will artificial intelligence change healthcare?, World Economic Forum: <https://www.weforum.org/agenda/2015/10/how-will-artificial-intelligence-change-healthcare>

Services à la clientèle

Plusieurs systèmes et logiciels ont été créés au cours des dernières années pour tenir une conversation ou autrement interagir avec les gens, que ce soit sous forme vocale ou celle de messages texte. Les entreprises utilisent ces logiciels dans le cadre de la prestation de services à leurs clients ou à des fins de divertissement, par exemple, dans des plateformes telles que Facebook, Messenger et Snapchat. Bien que ces logiciels ne soient pas nécessairement des applications absolues d'intelligence artificielle, quelques-unes de leurs caractéristiques courantes ou en voie de perfectionnement sont considérées comme de l'intelligence artificielle.

Lorsque ces logiciels sont utilisés pour conclure des contrats (aux fins, par exemple, d'effectuer des achats ou de passer des commandes ou encore de confirmer un consentement), il est important de s'assurer que les modalités applicables à ces contrats ou, le cas échéant, un avis d'exclusion de responsabilité valide soient communiquées à l'utilisateur. Cette utilisation de logiciels et de systèmes d'intelligence artificielle soulèvera inévitablement des questions intéressantes quant à la formation du contrat, sa nature et ses effets.



Secteur financier et technologies financières (ou « fintech »)

On remarque une recrudescence importante des activités de recherche et de développement dans les domaines de la robotique, de l'informatique et des technologies en lien avec les services financiers et des fintech. Les applications de l'intelligence artificielle dans ce domaine varient grandement et incluent l'analyse comportementale des clients et des investisseurs ainsi que l'analyse de multiples mégadonnées visant à améliorer la compréhension des consommateurs et des investisseurs, les stratégies de placements et l'utilisation des instruments dérivés.

Les défis juridiques que présente l'intelligence artificielle au cœur des secteurs financiers et économiques pourraient découler, par exemple, des conséquences du mauvais fonctionnement d'algorithmes. Dans un tel cas, la relation constante entre l'intervention humaine et les systèmes d'intelligence artificielle, notamment dans le cadre d'une plateforme de négociation de titres ou d'actions, devra être analysée et administrée soigneusement de façon à éviter certains risques juridiques ou, à tout le moins, les confiner à certains aspects plus spécifiques.



Véhicules autonomes

Les véhicules autonomes sont également désignés des voitures sans conducteur, bien qu'en pratique les véhicules autorisés à circuler sur la voie publique ne soient pas complètement autonomes. En juin 2011, l'État du Nevada devenait un des premiers territoires au monde à permettre que des véhicules autonomes circulent sur la voie publique. En vertu des lois du Nevada, un véhicule autonome est un (traduction libre) « véhicule qui est doté d'intelligence artificielle et de technologie permettant au véhicule d'exécuter toutes les opérations mécaniques associées à la conduite sans le contrôle actif ou la surveillance continue d'une personne physique »⁵.

Le Canada n'a toujours pas adopté de loi pour encadrer de telles voitures sans conducteur bien que plusieurs discussions ont cours à ce sujet. Parmi les importants défis juridiques qui se posent à l'égard des véhicules autonomes, soulignons les multiples questions de responsabilité et d'assurance. En effet, lorsqu'une voiture se déplace sans conducteur et qu'un accident survient, qui devrait être tenu responsable? Nous anticipons également que des arguments intéressants seront débattus relativement aux voitures sans conducteur dans le cadre d'activités commerciales dans le domaine des transports, notamment l'envoi et la livraison de marchandises commerciales.

⁵ Nevada Administrative Code Chapter 482A-Autonomous Vehicles, NAC 482A.010: <http://www.leg.state.nv.us/NAC/NAC-482A.html>

Responsabilité civile et contractuelle

La nature fondamentale des technologies de l'intelligence artificielle constitue un défi en soi en matière de responsabilité contractuelle et extra contractuelle. Lorsqu'une machine prend, ou prétend pouvoir prendre, des décisions autonomes sur la foi de données à la fois fournies par ses utilisateurs et acquises de façon autonome par la machine, son rendement ainsi que les résultats finaux pourraient s'avérer imprévisibles.

Ayant ce contexte à l'esprit, la lecture du Livre Cinquième du Code civil du Québec sur les obligations nous apporte un certain nombre de réflexions juridiques intéressantes eu égard aux nouveautés anticipées en matière d'intelligence artificielle :

- L'article 1457 du Code civil du Québec énonce que « Toute personne a le devoir de respecter les règles de conduite qui, suivant les

circonstances, les usages ou la loi, s'imposent à elle, de manière à ne pas causer de préjudice à autrui. Elle est, lorsqu'elle est douée de raison et qu'elle manque à ce devoir, responsable du préjudice qu'elle cause par cette faute à autrui et tenue de réparer ce préjudice, qu'il soit corporel, moral ou matériel. Elle est aussi tenue, en certains cas, de réparer le préjudice causé à autrui par le fait ou la faute d'une autre personne ou par le fait des biens qu'elle a sous sa garde. »

- L'article 1458 du Code civil du Québec énonce en outre que « Toute personne a le devoir d'honorer les engagements qu'elle a contractés. Elle est, lorsqu'elle manque à ce devoir, responsable du préjudice, corporel, moral ou matériel, qu'elle cause à son cocontractant et tenue de réparer ce préjudice ; ni elle ni le cocontractant ne peuvent alors se soustraire

à l'application des règles du régime contractuel de responsabilité pour opter en faveur de règles qui leur seraient plus profitables. »

- Aux termes de l'article 1458 du Code civil du Québec, « Le gardien d'un bien est tenu de réparer le préjudice causé par le fait autonome de celui-ci, à moins qu'il prouve n'avoir commis aucune faute ».

Les questions entourant les dommages prévisibles ou directs, selon le régime de responsabilité applicable, ou encore découlant du « fait autonome » d'un bien considéré comme un produit d'intelligence artificielle vont inévitablement soulever des débats intéressants dans le contexte de la mise au point des applications d'intelligence artificielle dans un avenir très rapproché. Dans quelles circonstances les concepteurs ou fournisseurs d'applications d'intel-

ligence artificielle, les utilisateurs et les autres parties bénéficiant de ces applications engageront-ils leur responsabilité à l'égard des résultats dérivant de celles-ci ou de l'utilisation de ces résultats par diverses personnes? Encore ici, l'interaction entre l'intervention humaine et les systèmes d'intelligence artificielle (ou l'absence d'une telle interaction dans certaines cas!) dans le cadre des diverses étapes associées à la production de biens ou la fourniture de services jouera un rôle déterminant dans la façon dont cette responsabilité sera établie.

Parmi les questions demeurant sans réponse en matière de responsabilité, est-ce que les systèmes autonomes utilisant des applications d'intelligence artificielle pourraient à un certain moment être tenus « personnellement » responsables des conséquences de leurs gestes? Et dans quelles

Responsabilité civile et contractuelle

situations le législateur devra-t-il combler certains vides juridiques découlant de l'absence de règles claires qui risquent de compromettre les droits et les obligations de toutes les parties qui interagissent avec l'intelligence artificielle? Plusieurs parallèles pourront être établis avec d'autres situations menant à la détermination de la responsabilité civile ou contractuelle des personnes. Notre jurisprudence a traité des cas de toute sorte dans ce domaine, mais force est de constater que les caractéristiques propres aux produits d'intelligence artificielle susciteront leur lot de réflexions complexes dans ce domaine.

Il est intéressant de rappeler qu'en janvier 2017, la Commission des affaires juridiques de l'Union européenne a soumis une proposition par laquelle elle demande l'adop-

tion de lois traitant de questions liées à la robotique. Dans le cadre des recommandations de la Commission, une réforme du droit de la responsabilité a été considérée comme essentielle. Il fut en effet recommandé que (traduction libre) « le futur texte législatif devrait prévoir des dispositions imposant l'application de la responsabilité stricte, faisant en sorte que tout ce qui devrait être prouvé est qu'un dommage est survenu, de même que le lien de causalité entre l'acte dommageable d'un robot et le dommage causé à la partie lésée »⁶. La Commission suggère en outre que le Parlement Européen étudie la possibilité d'imposer un régime d'assurance obligatoire ou l'établissement d'un fonds de compensation pour assurer que les victimes de système robotiques soient dédommagées.

⁶ Committee on Legal Affairs, Draft report with recommendations to the Commission on Civil Law Rules on Robotics, article 27. (2015/2103 (INL))

Que nous réserve l'avenir en matière d'intelligence artificielle?

À une époque où les chercheurs, les développeurs et les scientifiques effectuent des percées dans le domaine de l'intelligence artificielle à une vitesse incroyable et ce, dans divers domaines et sciences, appuyés dans plusieurs cas par des fonds et des subventions des gouvernements, certains concepts juridiques devront inévitablement être adaptés pour faire face aux défis que ces percées amèneront. Il est essentiel d'être conscient des risques juridiques associés aux importantes percées dans le domaine de l'intelligence artificielle et de prendre des décisions éclairées dans le cadre de la gestion du développement et de l'utilisation de l'intelligence artificielle.

L'intelligence artificielle devra apprendre à écouter, à comprendre et à distinguer de multiples concepts et idées, même sans le soutien d'opinions prédéfinies ou de ba-

lises formelles, de façon à acquérir des capacités d'anticipation et d'autres fonctions cognitives de la même façon que le font les êtres humains (même si d'aucuns pourraient prétendre que l'écoute et la compréhension demeurent des tâches difficiles même pour les humains...).

À un certain moment dans leur évolution, les systèmes d'intelligence artificielle prendront leur élan et cet élan s'accélérera lorsque deux systèmes ou plus d'intelligence artificielle combineront leurs fonctionnalités pour créer un système « supérieur » d'intelligence artificielle. La grande question est donc de savoir qui entreprendra avec succès cette combinaison astucieuse de deux systèmes ou plus, nous les humains ou les systèmes d'intelligence artificielle eux-mêmes?

Intelligence artificielle : les obligations contractuelles au-delà de l'expression à la mode

Par : **Eric Lavallée**

*Responsable du Laboratoire
juridique Lavery sur l'intelligence
artificielle (L³IA)*

Est-ce qu'un ordinateur peut apprendre et être intelligent? Dans l'affirmative, quelles sont les limites des tâches qu'on peut lui confier? Ces questions ont fait l'objet d'innombrables débats depuis au moins aussi longtemps que la publication d'Alan Turing sur les nombres calculables en 1937¹. De nombreux chercheurs se sont consacrés à développer des méthodes permettant aux ordinateurs d'interagir plus facilement avec les êtres humains et d'intégrer des processus leur servant à apprendre des situations qui se sont présentées. En quelque sorte, on souhaite permettre à la machine de penser et de réagir comme le ferait un être humain. Dès le début des années 1960, Marvin Minsky, célèbre chercheur du MIT, répertoriait ce qu'il considérait comme les étapes

devant mener au développement d'une intelligence artificielle². La puissance des ordinateurs récents ainsi que la capacité d'emmagasiner des quantités phénoménales d'information permettent aujourd'hui d'intégrer l'intelligence artificielle en entreprise et dans la vie quotidienne, souvent sous les vocables d'apprentissage automatique (machine learning), d'exploration des données (data mining) ou d'apprentissage profond (*deep learning*) — cette dernière forme ayant connu un développement fulgurant au cours des dernières années³.

L'utilisation de l'intelligence artificielle en entreprise soulève toutefois de nombreuses questions juridiques. Ces enjeux sont d'importance capitale lorsque des

¹ Turing, A. M. (1937). On computable numbers, with an application to the Entscheidungsproblem. *Proceedings of the London mathematical society*, 2(1), 230-265.

² Minsky, M. (1961). Steps toward artificial intelligence. *Proceedings of the IRE*, 49(1), 8-30.

³ Voir notamment : LeCun, Y., Bengio, Y., & Hinton, G. (2015). Deep learning. *Nature*, 521(7553), 436-444.

entreprises concluent des contrats pour offrir ou recevoir des produits et services dans le domaine de l'intelligence artificielle. En matière contractuelle, il est important de bien encadrer les obligations de chaque partie ainsi que leurs attentes.

Pour les fournisseurs de produits d'intelligence artificielle, un enjeu important est la responsabilité qu'ils encourent en cas de dysfonctionnement de leurs produits. À titre d'exemple, est-ce que les concepteurs d'un système d'intelligence artificielle pour l'aide à la décision dans un contexte médical peuvent être tenus responsables, directement ou indirectement, de l'erreur médicale découlant d'informations ou de suggestions erronées données par ce système? Il peut être opportun de s'assurer que les contrats exigent spécifiquement des professionnels utilisant

de tels systèmes qu'ils exercent un certain contrôle sur les résultats, que ce soit en médecine, en ingénierie ou en gestion des affaires.

En contrepartie, les entreprises qui désirent utiliser de tels produits doivent encadrer clairement les objectifs qu'ils souhaitent ainsi atteindre. Il ne s'agit pas là d'une simple question de performance du système d'intelligence artificielle, mais aussi de prévision de ce qui constituerait une défaillance des produits et ses conséquences juridiques. Par exemple, l'utilisation d'intelligence artificielle dans la gestion de la production d'une entreprise doit elle permettre une augmentation du rendement ou une diminution de certains problèmes? Qu'arrive-t-il si les performances souhaitées ne sont pas atteintes?

Un autre enjeu important est la propriété intellectuelle des données intégrées et générées par le produit d'intelligence artificielle. Plusieurs systèmes d'intelligence artificielle nécessitent l'utilisation d'un grand volume de données de l'entreprise afin que ces systèmes acquièrent l'« expérience » nécessaire à leur apprentissage. Toutefois, à qui appartiennent ces données et à qui appartiendront les résultats de cet apprentissage par le système d'intelligence artificielle? Par exemple, pour qu'un système d'intelligence artificielle puisse devenir performant, une entreprise pourrait se voir obligée de lui soumettre une grande quantité de données et d'investir des ressources humaines ainsi que financières considérables pour guider son apprentissage. Est-ce que le fournisseur du système d'intelligence artificielle acquiert des droits sur ces données? Est-ce qu'il peut se servir de l'apprentissage de son système d'intelligence

artificielle dans une entreprise pour en faire bénéficier ses autres clients? Dans des cas extrêmes, cela pourrait faire en sorte que l'expérience acquise par un système au sein d'une entreprise bénéficie aux concurrents de cette dernière.

Lorsque le système d'intelligence artificielle est utilisé dans des applications visant des consommateurs ou les employés d'une entreprise, il ne faut pas négliger non plus les enjeux liés à la confidentialité des données utilisées par le système d'intelligence artificielle et à la protection de la vie privée de ces personnes.

Il s'agit là d'autant d'enjeux qui doivent être encadrés au point de vue contractuel avant que les problèmes ne surviennent.

Intelligence artificielle, implantation et ressources humaines

Par : **Dave Bouchard**

À l'ère d'une nouvelle révolution industrielle, surnommée industrie 4.0, les entreprises font face à des enjeux technologiques de taille. Certains parleront plutôt d'usine intelligente ou encore d'industrie du futur. Cette révolution est caractérisée par l'avènement de nouvelles technologies permettant, entre autres, une automatisation « intelligente » de l'activité humaine.

Cette révolution technologique a notamment pour visée d'augmenter la productivité, l'efficacité et la flexibilité des organisations. Il s'agit dans certains cas, d'un véritable bouleversement de la chaîne de valeurs de l'entreprise.

L'intelligence artificielle est partie intégrante de cette nouvelle ère. Cette notion qui existe déjà de-

puis le milieu des années 1950 se définit comme étant la simulation de l'intelligence humaine par des machines¹. L'intelligence artificielle vise à se substituer à presque toutes les tâches actuellement effectuées par des êtres humains, à les compléter ou à les amplifier². Elle constitue en quelque sorte le concurrent tout désigné de l'être humain sur le marché de l'emploi. L'avènement dans les dernières années de l'apprentissage profond et d'autres techniques avancées d'apprentissage des machines et ordinateurs a permis de faire apparaître de nombreuses applications en milieu industriel qui ont le potentiel de révolutionner la manière d'organiser le travail dans les entreprises.

¹ Encyclopédie Larousse en ligne

² Spyros Makridakis, The Forthcoming Artificial Intelligence (AI) Revolution: Its Impact on Society and Firms, School of Economic Sciences and Business, Neapolis University Paphos, 2017



On estime que l'intelligence artificielle pourrait contribuer à faire augmenter le PIB mondial de 14 % d'ici 2030 pour générer annuellement un potentiel de 15 700 milliards de dollars de gains pour l'économie mondiale³. Les gains en productivité au travail créés par l'intelligence artificielle pourraient représenter à eux seuls plus de la moitié de cette somme. Il va sans dire que le marché du travail devra assurément s'y adapter.

D'ailleurs, une étude publiée il y a quelques années prédisait que d'ici vingt ans, près de 50 % des emplois aux États-Unis seraient, en partie ou en totalité, susceptibles d'être automatisés⁴. En 2016, une étude de l'OCDE concluait plutôt qu'en moyenne, dans les 21 pays de l'OCDE, plus ou moins 9 % des emplois seraient en totalité à haut risque d'automatisation⁵. Sans compter que certains auteurs vont même jusqu'à prétendre qu'environ 85 % des emplois qui seront exercés en 2030 n'existent pas encore aujourd'hui⁶!

À tout le moins, ces données permettent de constater que les êtres humains demeureront indispensables, mais que le marché du travail sera grandement transformé par l'intelligence artificielle. Que ce soit en raison de la transformation de tâches, de la disparition d'emplois ou encore de la création de nouveaux métiers, des bouleversements sont à prévoir dans les milieux de travail et les entreprises devront y faire face.

L'arrivée de l'intelligence artificielle semble donc être inévitable. Dans certains cas, cette technologie permettra de créer un avantage concurrentiel important. Les entreprises innovantes s'y démarqueront. Cependant, en plus des investissements majeurs qui seront nécessaires, l'implantation de ce nouvel outil technologique exigera du temps, des efforts et plusieurs changements dans les méthodes de travail.

³ Sizing the prize, PWC, 2017

⁴ Carl Benedikt Frey and Michael A. Osborne, *The future of employment: How susceptible are jobs to computerisation*, Oxford University, 2013

⁵ Melanie Arntz, Terry Gregory, Ulrich Zierahn, *The Risk of Automation for Jobs in OECD Countries*, OECD Social, Employment and Migration Working Papers, 2016

⁶ *Emerging Technologies' Impact on Society & Work in 2030*, Institute for the future and Dell Technologies, 2017

Implantation

À titre d'entrepreneur, vous devrez nécessairement vous adapter à cette nouvelle réalité. Non seulement vos employés seront affectés par ce changement organisationnel, mais ils devront en être également les principaux acteurs afin d'assurer la réussite de l'opération.

Au cours de l'exercice d'implantation, vous découvrirez peut-être que de nouvelles compétences sont désormais requises afin de s'ajuster à votre technologie. De plus, il y a de fortes probabilités que vous constatiez que certains de vos employés et gestionnaires adoptent une attitude réfractaire face à ce changement. Il s'agit là d'une réaction qui caractérise bien l'être humain, lequel a tendance à réagir négativement à tout type de

changement. Cette réaction s'explique, entre autres, par le fait que toute modification dans un environnement de travail est susceptible d'entraîner un sentiment d'insécurité, exigeant que les employés adoptent de nouveaux comportements ou de nouvelles méthodes de travail⁷. Cela met en péril le réconfortant statu quo. Sachez que bien souvent, les craintes de vos employés seront alimentées par des perceptions erronées.

Une réflexion s'impose donc, car il pourrait être sage de planifier les impacts potentiels avant même que votre nouvelle technologie atterrisse dans votre entreprise.

À cet égard, on évalue le taux d'échec en matière de changement organisationnel à plus de 70 %. En ce qui a trait à l'implantation d'une nouvelle technologique, on estime que ce haut taux d'échec s'explique par le fait que l'aspect humain est souvent sous-estimé aux profits de l'aspect technique ou opérationnel que requiert l'implantation de la technologie⁸. Un échec peut amener des coûts plus élevés pour l'introduction de votre nouvel outil, des pertes de productivité ou tout simplement l'abandon complet de l'initiative. C'est pourquoi il vous

faudra mettre une attention particulière sur la planification avant l'implantation de votre intelligence artificielle afin de bien déceler les enjeux liés à son intégration dans votre entreprise.

Il sera important de confier l'implantation de cette technologie intelligente à des employés compétents qui partagent les valeurs de l'entreprise, afin d'éviter que le système implanté ne perpétue des comportements non désirables.

⁷ Simon L. Dolan, Éric Gosselin et Jules Carrière, *Psychologie du travail et comportement organisationnel*, 4^e éd., Gaétan Morin Éditeur, 2012

⁸ Yves-Chantal Gagnon, *Les trois leviers stratégiques de la réussite du changement technologique*, *Télescope - Revue d'analyse comparée en administration publique*, École nationale d'administration publique du Québec, automne 2008

Pour vous aider dans cette planification, voici quelques questionnements qui vous permettra d'entreprendre votre réflexion en la matière :

Implantation

- Quel est l'objectif de la nouvelle technologie, ses avantages et inconvénients ?
- Quel gestionnaire sera responsable du projet ?
- Quelles compétences seront nécessaires pour implanter cette technologie dans l'organisation ?
- Quels employés seront responsables d'implanter la technologie ?
- Quelles informations et formations devront leur être données ?

Organisation du travail

- Quelles tâches seront remplacées ou transformées par la nouvelle technologie et comment seront-elles transformées ?
- Quelles nouvelles tâches seront créées à la suite de l'arrivée de cette nouvelle technologie ?
- Y aura-t-il des abolitions de poste, des mouvements de main-d'œuvre et des pertes d'emploi ?
- Quelles dispositions de la convention collective devront être respectées notamment en matière de mouvements de main-d'œuvre, de mise à pied et de changement technologique ?
- Quels sont les préavis et les indemnités à prévoir en cas de pertes d'emploi ?
- Quels postes devront être créés à la suite de l'arrivée de cette technologie ?
- Quelles sont les nouvelles compétences requises pour ces postes ?
- Comment seront pourvus ces nouveaux postes et quand le seront-ils ?
- Comment les utilisateurs de cette technologie devront-ils être entraînés et formés ?

Communication

- Qui sera responsable de la communication ?
- Devrez-vous mettre en place des outils de communication et un plan de communication ?
- Sous quelles formes se fera cette communication et à quelle fréquence ?
- Quand et comment les employés et gestionnaires seront-ils informés de l'arrivée de la nouvelle technologie, de l'objectif de cette implantation, ses avantages et les impacts pour l'organisation ?
- Quand et comment seront annoncés les pertes d'emploi, les mouvements de main-d'œuvre et les nouveaux postes ?
- Quels seront les outils utilisés pour rassurer vos employés et éliminer les perceptions erronées ?

Mobilisation

- Quels gestes et actions peuvent être pris pour assurer la mobilisation des employés et gestionnaires dans ce projet ?
- Quelles seront les réactions probables au changement et comment pouvons-nous les atténuer ou les éliminer ?
- Comment outiller les gestionnaires dans la gestion de ce changement ?

Évidemment, cette liste n'est pas exhaustive, mais elle peut vous servir de point de départ pour alimenter votre réflexion relativement aux impacts potentiels de votre nouvelle technologie intelligente sur vos employés. Rappelez-vous qu'une bonne gestion de la communication avec vos employés et la mobilisation de ceux-ci seront assurément des facteurs de réussite de ce changement technologique.

La propriété intellectuelle de l'intelligence artificielle

Par : **Eric Lavallée**

*Responsable du Laboratoire
juridique Lavery sur l'intelligence
artificielle (L³IA)*

Bien que l'intelligence artificielle soit en constante évolution depuis quelques années, le droit peine parfois à s'y adapter. Les enjeux de propriété intellectuelle sont particulièrement importants : il faut en effet s'assurer que les entreprises qui investissent dans ces technologies puissent profiter pleinement de leurs retombées commerciales. Le présent bulletin constitue un survol des diverses formes de propriété intellectuelle qui peuvent s'avérer pertinentes en matière d'intelligence artificielle.

Le premier réflexe de nombreux entrepreneurs est souvent de vouloir breveter leurs procédés d'intelligence artificielle. Toutefois, bien qu'il s'agisse d'un mode de pro-

tection qui puisse être envisagée dans certains cas, l'obtention d'un brevet ne constitue pas nécessairement la forme de protection la plus adaptée à l'intelligence artificielle ou aux technologies logicielles en général. En effet, depuis l'importante décision de la Cour Suprême des États Unis dans l'affaire *Alice Corp. v. CLS Bank*¹ *International*, il est reconnu que le fait d'appliquer des idées abstraites à l'environnement informatique n'est pas suffisant pour transformer ces idées en objets brevetables. Par exemple, un brevet pourtant émis pour un système expert, constituant une forme d'intelligence artificielle, a été invalidé par les tribunaux américains à la suite de cette décision².

¹ 573 U.S. ___, 134 S. Ct. 2347 (2014).

² *Vehicle Intelligence and Safety v. Mercedes-Benz*, 78 FSupp.3d 884 (2015), maintenue en appel Federal Circuit No. 2015-1411 (U.S.).

Au Canada, la jurisprudence n'a pas encore traité de cas spécifique aux systèmes d'intelligence artificielle. Par contre, nul doute que les principes dégagés par la cour d'appel fédérale dans la décision *Schlumberger Canada Ltd. c. Commissaire des brevets*³ demeurent pertinents. Dans cette affaire, il a été décidé qu'un procédé permettant de recueillir, d'enregistrer et d'analyser des données à l'aide d'un ordinateur qui appliquait alors une formule mathématique ne pouvait faire l'objet d'un brevet. Par contre, dans une décision plus récente, la cour en est venu à la conclusion qu'un procédé informatique pourrait être brevetable s'il « [...] ne constitue pas l'invention entière, mais seulement un élément essentiel parmi d'autres dans une nouvelle combinaison. »⁴

Il est donc à prévoir qu'un algorithme d'intelligence artificielle pris isolément ne pourra faire l'objet d'un brevet.

Quant à l'Europe, en vertu de l'Article 52 de la Convention sur le brevet européen de 1973, les programmes d'ordinateurs ne sont pas brevetables. Il est donc impossible d'obtenir un brevet sous ce régime pour la programmation sous-jacente à un système d'intelligence artificielle.

Le droit d'auteur est peut-être la plus évidente des formes de propriété intellectuelle en ce qui concerne l'intelligence artificielle. En effet, les codes sources sont reconnus depuis longtemps comme étant des œuvres au sens de la *Loi sur le droit d'auteur* canadienne de

même que par des lois similaires dans la plupart des pays. Certains pays ont même adoptés des lois s'appliquant précisément à la protection des logiciels⁵.

Une décision canadienne plus ancienne présente en outre un intérêt : *Apple Computer, Inc. c. Mackintosh Computers Ltd.*⁶ On y indique qu'un algorithme incorporé dans un circuit ROM (read only memory) est considéré comme étant une œuvre protégée par le droit d'auteur. Une décision semblable avait été rendue aux États-Unis précédemment⁷. Dans le cas d'un système d'intelligence artificielle, ces décisions sont importantes en ce qu'elles étendent la protection du droit d'auteur non seulement au code étant programmé dans des langages de haut niveau ou sur des plateformes

d'intelligence artificielles avancées, mais aussi au code objet en découlant, même sur un support électronique comme un circuit ROM. Le droit d'auteur ne protège toutefois pas les idées ou les principes généraux d'un code, mais bien leur expression.

D'autre part, il ne faut pas sous-estimer la protection que confèrent les secrets industriels. Plus particulièrement, en matière d'informatique, rares sont les clients qui ont accès à l'ensemble du code source. De plus, les codes sources en matière d'intelligence artificielle sont d'une certaine complexité qui contribue à cette protection⁸.

Il s'agit là d'une approche particulièrement intéressante pour les entreprises qui offrent des logiciels en tant que service à distance. En

³ [1982] 1 C.F. 845 (C.A.F.).

⁴ *Canada (Procureur général) c. Amazon.com, inc.*, [2012] 2 R.C.F. 459, 2011 CAF 328.

⁵ À titre d'exemple, au Bésil : *Lei do Software* No. 9.609 du 19 Février, 1998; en Europe : *Directive 2009/24/CE concernant la protection juridique des programmes d'ordinateur*.

⁶ [1990] 2 R.C.S. 209, 1990 CanLII 119 (C.S.C.).

⁷ *Apple Computer, Inc. v. Franklin Computer Corp.*, 714 F.2d 1240 (3d Cir. 1983) (U.S.).

⁸ Keisner, A., Raffo, J., & Wunsch-Vincent, S. (2015). *Breakthrough technologies - Robotics, innovation and intellectual property* (No. 30). World Intellectual Property Organization-Economics and Statistics Division.

effet, dans un tel cas, les clients n'ont accès qu'à l'interface, mais jamais au code source ni même au code compilé. Il est presque impossible d'en faire une réelle ingénierie inversée.

Toutefois, le risque encouru dans le cas où un système d'intelligence artificielle n'est protégé qu'en vertu de la notion de secret industriel est qu'une fuite originant d'un ou plusieurs employés permette à des concurrents de prendre connaissance du code source, de sa structure ou de ses particularités. On n'a qu'à s'imaginer comment il deviendrait difficile de rattraper une fuite de code source qui circulerait sur Internet. Il est bien sûr possible de faire signer des ententes de confidentialité, mais cela n'est malheureusement pas suffisant face à des employés de mauvaise foi ou

l'espionnage industriel. Il est donc opportun de mettre en place des mesures de fractionnement des connaissances au sein de l'entreprise, de sorte que très peu d'employés aient accès à l'ensemble de l'information critique.

Accessoirement, il pourrait être stratégique pour un fournisseur d'intelligence artificielle de s'assurer que ses clients mettent en évidence sa marque de commerce, à la manière de la stratégie de mise en marché coopérative « *Intel Inside* », de façon à promouvoir son système auprès d'autres clients potentiels.

Dans le cas des systèmes d'intelligence artificielle utilisés vendus dans un contexte commercial, il est également important de considérer la propriété intellectuelle sur les résultats de l'apprentissage des

systèmes liés à l'utilisation qui en est faite. Il faut se demander si les bases de données qui sont générées par un système d'intelligence artificielle mis au point par un fournisseur de logiciel, à l'occasion de l'utilisation qu'en fait un de ses clients, appartiennent au fournisseur de logiciel ou à ce client. C'est souvent le contrat entre les parties qui régira cette situation. Toutefois, il peut être légitime pour une entreprise de vouloir conserver la propriété intellectuelle sur les bases de données qui sont générées par l'usage interne qu'elle fait du logiciel, notamment en lui soumettant ses données opérationnelles ou en « entraînant » le système d'intelligence artificielle au fil des interactions avec ses employés.

Le fait de vouloir conserver la confidentialité de ces bases de données découlant de l'usage de l'intelligence artificielle permet de les assimiler à des secrets industriels. Toutefois, la question de savoir s'il s'agit d'œuvres au sens du droit d'auteur devra être déterminée au cas par cas. Il faudra entre autre tenter d'établir si ces bases de données résultent d'un exercice de talent et de jugement d'un ou plusieurs auteurs, comme le veut la jurisprudence canadienne à cet égard⁹. Alors que les situations où des employés « entraînent » un système d'intelligence artificielle semblent plus facilement assimilables à un exercice de talent et de jugement de leur part, celles où des bases de données sont constituées de manière autonome

⁹ CCH Canadian Ltd. c. Law Society of Upper Canada, 2004 CSC 13, [2004] 1 RCS 339.

par le système risquent d'échapper au droit d'auteur, puisqu'il n'existe pas de droit d'auteur sur les données elles-mêmes¹⁰, mais bien sur leur analyse et leur compilation par un auteur.

En effet, à toutes ces questions s'ajoute celle, plus prospective, des inventions créées par des systèmes d'intelligence artificielle. Déjà, des systèmes d'intelligence artificielle sont utilisés pour répertorier des domaines de recherche présentant des occasions d'innovation. Par exemple, des systèmes d'exploration des données (data mining) sont déjà utilisés pour analyser les textes des brevets, découvrir des champs de recherche émergents

et même trouver des domaines conceptuels étant « disponibles » pour d'éventuels brevets¹¹. Il est possible que les systèmes d'intelligence artificielle puissent être utilisés au cours des prochaines années pour rédiger des demandes de brevet de manière automatisée, notamment pour en rédiger les revendications¹². L'intelligence artificielle pourrait-elle être titulaire de droits de propriété intellectuelle, par exemple sur des brevets ou des droits d'auteur? Nous en doutons, car les lois actuelles attribuent des droits aux inventeurs et créateurs en tant que personnes physiques, du moins au Canada et aux États-Unis¹³.

Mais alors, est-ce que la propriété intellectuelle de l'invention reviendrait aux concepteurs du système d'intelligence artificielle? Nous ne croyons pas non plus que le droit soit bien adapté à cet égard, la propriété intellectuelle étant historiquement accordée aux personnes ayant fait preuve d'inventivité en matière de brevet ou de l'exercice d'un talent et de jugement en matière de droit d'auteur, selon le cas. On peut se demander si on verra un brevet invalidé ou une œuvre tomber dans le domaine public au motif qu'une portion substantielle en est générée par l'intelligence artificielle (ce qui n'est pas le cas de ce bulletin!).

D'ici là, les juristes devront se familiariser avec les concepts sous-jacents de l'intelligence artificielle, tout comme les informaticiens devront se familiariser avec ceux de la propriété intellectuelle. Pour les entrepreneurs qui conçoivent ou utilisent des systèmes d'intelligence artificielle, une réflexion constante sur la propriété intellectuelle s'impose pour protéger le fruit de leurs efforts.

¹⁰ Voir par exemple: *Geophysical Service Incorporated c. Office Canada-Nouvelle-Écosse des hydrocarbures extracôtiers*, 2014 CF 450.

¹¹ Voir par exemple: Lee, S., Yoon, B., & Park, Y. (2009). An approach to discovering new technology opportunities: Keyword-based patent map approach. *Technovation*, 29(6), 481-497; Abbas, A., Zhang, L., & Khan, S. U. (2014). A literature review on the state-of-the-art in patent analysis. *World Patent Information*, 37, 3-13.

¹² Hattenbach, B., & Glucoft, J. (2015). Patents in an Era of Infinite Monkeys and Artificial Intelligence. *Stan. Tech. L. Rev.*, 19, 32.

¹³ *Supra*, note 7.

Lorsque l'intelligence artificielle est discriminatoire

Par : **Eric Lavallée**

*Responsable du Laboratoire
juridique Lavery sur l'intelligence
artificielle (L³IA)*

L'intelligence artificielle a connu des avancées importantes depuis quelques années, notamment grâce aux avancées de ce que l'on nomme maintenant l'apprentissage profond (deep learning)¹. Cette méthode est le prolongement des réseaux neuroniques qui sont utilisés depuis quelques années pour l'apprentissage des machines. L'apprentissage profond, comme toute forme d'apprentissage d'une machine, requiert que le système d'intelligence artificielle soit confronté à diverses situations afin d'apprendre à réagir à des situations présentant des similitudes à ces expériences antérieures.

En entreprise, des systèmes d'intelligence artificielle sont notamment utilisés pour répondre aux besoins des clients, soit directement, soit en soutenant les employés dans leurs interventions. La qualité des services rendus par l'entreprise est donc de plus en plus tributaire de la qualité de ces systèmes d'intelligence artificielle.

Il ne faut pas, toutefois, faire l'erreur de présumer qu'un tel système informatique s'acquittera automatiquement des tâches qui lui sont confiées sans faille et dans le respect des valeurs de l'entreprise ou de sa clientèle.

¹ LeCun, Y., Bengio, Y., & Hinton, G. (2015). Deep learning. *Nature*, 521(7553), 436-444.

Par exemple, des chercheurs de l'université Carnegie Mellon ont récemment démontré qu'un système devant présenter de la publicité ciblée à des usagers d'Internet offrait systématiquement moins de postes bien rémunérés aux femmes qu'aux hommes². En d'autres termes, ce système avait un comportement que l'on pourrait qualifier de sexiste. Bien que les chercheurs n'aient pu identifier l'origine du problème, ils étaient d'avis qu'il s'agissait probablement d'une perte de contrôle du fournisseur de service de placement de publicité sur son système automatisé, et ils soulignaient les risques inhérents aux systèmes d'intelligence artificielle à grande échelle.

Divers systèmes d'intelligence artificielle ont connu des ratés similaires, démontrant des comportements racistes et forçant même un exploitant à suspendre l'accès à son système³.

À cet égard, l'Union Européenne a adopté env avril 2016 une réglementation relative au traitement de l'information personnelle qui, sauf dans certains cas précis, interdit la prise de décision automatisée basée sur certaines données à caractère personnel, dont « [...] l'origine raciale ou ethnique, les opinions politiques, les convictions religieuses ou philosophiques ou l'appartenance syndicale, ainsi que le traitement des données génétiques, des données biométriques

aux fins d'identifier une personne physique de manière unique, des données concernant la santé ou des données concernant la vie sexuelle ou l'orientation sexuelle d'une personne physique [...] »⁴. Certains chercheurs s'interrogent d'ailleurs sur l'application de ce règlement, notamment alors que la discrimination apparaît de manière incidente, hors la volonté de l'exploitant du système d'intelligence artificielle⁵.

Au Québec, on peut croire qu'une entreprise qui exploiterait un système d'intelligence artificielle discriminatoire au sens des lois applicables ou de la Charte des droits et libertés de la personne s'exposerait à des recours, même en l'absence de règlement précis comme celui de l'Union Européenne. En effet, le responsable du bien qu'est ce système d'intelligence artificielle pourrait voir sa responsabilité engagée à l'égard du préjudice ou du dommage causé par le fait autonome de ce bien. Qui plus est, le fait de ne pas mettre en place des

² Datta, A., Sen, S., & Zick, Y. (2016, May). Algorithmic transparency via quantitative input influence: Theory and experiments with learning systems. In *Security and Privacy (SP), 2016 IEEE Symposium on* (pp. 598-617). IEEE; Datta, A., Tschantz, M. C., & Datta, A. (2015). Voir aussi: Automated experiments on ad privacy settings. *Proceedings on Privacy Enhancing Technologies*, 2015(1), 92-112.

³ Reese, H. (2016). Top 10 AI failures of 2016. Repéré à <http://www.techrepublic.com/article/top-10-ai-failures-of-2016/>. Le cas de *Tay*, le système de Microsoft, a été abondamment discuté dans les médias.

⁴ Règlement (UE) 2016/679 du parlement européen et du conseil du 27 avril 2016, relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données), art. 22.

⁵ Goodman, B., & Flaxman, S. (2016, June). EU regulations on algorithmic decision-making and a «right to explanation». In *ICML Workshop on Human Interpretability in Machine Learning (WHI 2016)*.

mesures raisonnables pour éviter la discrimination serait fort probablement pris en compte dans l'analyse juridique d'une telle situation.

Une vigilance particulière s'impose donc lorsque le fonctionnement d'un système d'intelligence artificielle repose sur des données déjà accumulées au sein de l'entreprise, des données de tiers (notamment ce qu'on désigne souvent comme le big data), ou encore lorsque les données seront fournies au système d'intelligence artificielle par des employés de l'entreprise ou ses utilisateurs au cours d'une période « d'apprentissage ». Toutes ces sources de données, par ailleurs soumises aux obligations découlant des lois applicables à la protection des renseignements personnels, peuvent être biaisées à divers degrés.

Les effets d'un échantillonnage biaisé ne sont pas nouveaux ni cantonnés au respect des droits de la personne. Il s'agit d'un effet bien connu des statisticiens. Pendant la Seconde Guerre mondiale, la marine américaine demanda à un mathématicien nommé Abraham Wald de leur fournir des statistiques sur les parties des avions bombardiers ayant été les plus touchés dans le but de renforcer le blindage à ces endroits. Wald démontra que les données sur les avions revenant de mission étaient biaisées, car elles ne tenaient pas compte des avions abattus en mission. Il ne fallait donc pas renforcer le blindage sur les parties où les avions revenant de mission étaient endommagés, mais plutôt aux endroits où ils n'étaient pas touchés.

Dans le contexte de l'exploitation d'une entreprise, un système d'intelligence artificielle auquel on soumet des données biaisées pourrait ainsi prendre des décisions erronées, ayant des conséquences néfastes au point de vue humain, économique et opérationnel pour l'entreprise.

Par exemple, si l'on soumet un tel système à un apprentissage encadré par des employés de l'entreprise, leur façon d'agir se reflétera sans doute dans son comportement ultérieur. Ceci peut se refléter dans les jugements portés par le système d'intelligence artificielle à l'égard de demandes de clients,

mais aussi directement dans leur capacité de résoudre adéquatement les problèmes techniques qui lui sont soumis. On risque ainsi de perpétuer les comportements problématiques de certains employés. Des chercheurs du Machine Intelligence Research Institute ont proposé diverses approches pour minimiser les risques et rendre l'apprentissage machine d'un système d'intelligence artificielle conforme aux intérêts de son exploitant⁶. Selon ces chercheurs, il pourrait notamment être opportun d'adopter une approche prudente quant aux objectifs imposés à de tels systèmes pour éviter qu'ils offrent des solutions extrêmes ou

⁶ Taylor, J., Yudkowsky, E., LaVictoire, P. & Critch, A. (2016). *Alignment for advanced machine learning systems*. Technical Report 2016, MIRI.

indésirables. Il serait en outre important d'établir des procédures de supervision informée, au moyen desquelles un opérateur peut s'assurer que le fonctionnement du système d'intelligence artificielle est, dans son ensemble, conforme aux attentes de son exploitant.

De ce qui précède, il faut retenir qu'une entreprise qui désire intégrer un système d'intelligence artificielle dans ses opérations doit prendre très au sérieux la phase d'implantation, au cours de laquelle se déroulera l'apprentissage

du comportement désiré par le système. D'une part, il sera important d'avoir des discussions approfondies avec le fournisseur sur le fonctionnement de sa technologie et ses performances, ainsi que d'encadrer contractuellement et le plus clairement possible les attentes de l'entreprise à l'égard du système qu'elle désire implanter. Il faut également prévoir comment s'effectuera l'intégration du système d'intelligence artificielle dans l'entreprise et s'assurer que cette intégration soit confiée à des employés et consultants dignes de

confiance, possédant le plus haut niveau de compétence eu égard aux tâches pertinentes.

Quant au fournisseur du système d'intelligence artificielle, il faudra généralement s'assurer que les données qui lui sont fournies ne sont pas biaisées, inexactes ou autrement altérées, de telle façon que les objectifs prévus au contrat quant aux performances souhaitées du système puissent raisonnablement être atteints, permettant ainsi de minimiser le risque de

litiges devant les tribunaux découlant de comportements discriminatoires ou défaillants à d'autres égards du système d'intelligence artificielle. Non seulement de tels litiges pourraient-ils s'avérer onéreux, ils seraient de surcroît susceptibles d'entacher tant la réputation du fournisseur que celle du client utilisateur.

Intelligence artificielle et chaînes de blocs : vulnérables aux cyberattaques

Par : **Eric Lavallée**

*Responsable du Laboratoire
juridique Lavery sur l'intelligence
artificielle (L³IA)*

Les technologies qui reposent sur les chaînes de blocs (blockchain en anglais) et l'intelligence artificielle représentent un changement important pour notre société. La sécurité des données qui y sont échangées étant cruciale, l'adoption de ces solutions doit être planifiée dès aujourd'hui dans une optique à long terme.

Les entreprises sont nombreuses à mettre au point des services qui reposent sur les chaînes de blocs, notamment dans le secteur des services financiers. Les cryptomonnaies, un exemple d'utilisation des chaînes de blocs, changent la manière dont s'effectuent certains échanges monétaires, loin du contrôle des institutions bancaires et des gouvernements.

Du côté de l'intelligence artificielle, les entreprises choisissent parfois des plateformes technologiques qui mettent en cause un partage des données dans le but d'accélérer la mise au point de leur outil d'intelligence artificielle.

L'impact de la révolution quantique sur la cybersécurité

En 2016, IBM a rendu accessible aux chercheurs un ordinateur permettant d'effectuer des essais sur divers algorithmes quantiques¹. Il faut savoir que le mode de fonctionnement des ordinateurs quantiques est radicalement différent de celui des ordinateurs conventionnels. D'ici une dizaine d'années, ils permettront d'effectuer rapidement des calculs qui dépassent la capacité des ordinateurs actuels les plus puissants. En effet, les ordinateurs quantiques utilisent les propriétés quantiques de la matière, notamment la superposition d'états, qui permet de traiter simultanément des ensembles de données liées.

L'algorithme de Shor est un algorithme utilisant des propriétés quantiques de la matière et qui peut être utilisé par des ordinateurs quantiques.

L'algorithme de Shor permet à un ordinateur quantique de factoriser un nombre entier très rapidement, beaucoup plus que n'importe quel ordinateur conventionnel. Cette opération mathématique est l'élément essentiel permettant de déchiffrer l'information qui a été encryptée par plusieurs méthodes répandues en informatique. Cette technologie, qui intéresse les physiciens depuis longtemps, représente désormais un risque important pour la sécurité des données encryptées. Les données que l'on souhaite garder sécurisées et confidentielles présentent ainsi une vulnérabilité aux détournements à des fins non-autorisées.

¹ Communiqué de presse : *IBM Makes Quantum Computing Available on IBM Cloud to Accelerate Innovation* : <https://www-03.ibm.com/press/us/en/press-release/49661.wss>; voir aussi : Linke, Norbert M., et al. « Experimental comparison of two quantum computing architectures. » *Proceedings of the National Academy of Sciences* (2017): 201618020.



Méthodes d'encryptages de chaînes de blocs : assez sécurisées ?

Plusieurs méthodes d'encryptages existent aujourd'hui et plusieurs d'entre elles devront être renforcées pour maintenir la sécurité des données. Et il ne s'agit là que de quelques exemples de vulnérabilités aux ordinateurs quantiques.

1. Méthodes SHA-2 et SHA-3

Le National Institute of Standards and Technology (NIST) des États-Unis a émis des recommandations quant à la sécurité de diverses méthodes d'encryptage². Les méthodes SHA 2 et SHA-3, qui sont les algorithmes qui servent à assurer l'intégrité des chaînes de blocs en produisant un « hachage » des blocs précédents, devront être renforcées pour maintenir le même niveau de sécurité.

2. Méthodes de signature utilisées par les Bitcoins et d'autres cryptomonnaies

La cryptographie par courbes elliptiques est un ensemble de techniques cryptographiques qui utilisent une ou plusieurs propriétés de fonctions mathématiques qui décrivent les courbes elliptiques afin d'encrypter des données.

Selon le NIST, la cryptographie par courbes elliptiques deviendra inefficace. Ce qui est préoccupant, c'est qu'on parle ici de la méthode utilisée pour la signature de cryptomonnaies, dont le célèbre Bitcoin. Des recherches récentes indiquent que cette méthode présente une grande vulnérabilité à une attaque

par des ordinateurs quantiques, qui pourraient déjouer ces codes en moins de dix minutes d'ici quelques années³.

3. Algorithmes cryptographiques de type RSA

Les algorithmes cryptographiques de type RSA⁴, très répandus pour la communication de données par Internet, sont particulièrement vulnérables aux ordinateurs quantiques. Ceci pourrait notamment avoir un impact si de grandes quantités de données devraient être échangées entre plusieurs ordinateurs, par exemple pour alimenter des systèmes d'intelligence artificielle.

4. Des algorithmes cryptographiques plus sécuritaires

Le NIST reconnaît certaines approches qui sont plus sécuritaires. Un algorithme mis au point par Robert McEliece, mathématicien et professeur à Caltech, semble pouvoir résister à ces attaques⁵ pour le moment. À plus long terme, on peut espérer que la technologie quantique permette elle-même de générer des clés sécuritaires.

² Chen, Lily, et al. *Report on post-quantum cryptography*. US Department of Commerce, National Institute of Standards and Technology, 2016.

³ Aggarwal, Divesh, et al. « Quantum attacks on Bitcoin, and how to protect against them. » arXiv preprint arXiv:1710.10377 (2017).

⁴ Il s'agit ici de l'acronyme des trois concepteurs de ce type d'encryptations, Rivest, Shamir et Adleman.

⁵ Supra, note 2 ; voir aussi Dinh, Hang, Christopher Moore, and Alexander Russell. « McEliece and Niederreiter cryptosystems that resist quantum Fourier sampling attacks. » *Annual Cryptology Conference*. Springer, Berlin, Heidelberg, 2011. d'encryptations, Rivest, Shamir et Adleman.



Incidences juridiques et d'affaires en matière de protection des données

La loi impose aux entreprises l'obligation de protéger les renseignements personnels et confidentiels qui leurs sont confiés par leurs clients. Elles doivent donc prendre des mesures adéquates pour protéger cet or brut que représentent les données.

Le choix d'une technologie d'intelligence artificielle ou de chaînes de blocs doit donc être effectuée dès aujourd'hui, en tenant compte du fait qu'une fois adoptée, celle-ci sera utilisée pendant plusieurs années et sera possiblement appelée à survivre à l'arrivée des ordinateurs quantiques.

Qui plus est, il faudra également corriger les failles de sécurité des technologies n'étant pas sous le contrôle d'autorités gouvernementales ou d'une seule entreprise.

Contrairement aux technologies plus conventionnelles, il ne s'agit pas d'installer une simple mise à jour sur un serveur unique. Dans certains cas, il faudra repenser la structure même d'une technologie décentralisée, telle la chaîne de blocs.

Faire le choix d'une technologie qui évolue

La clé sera donc de choisir une technologie qui permettra aux entreprises de respecter leurs obligations en matière de sécurité dans un monde post-quantique, ou à tout le moins de choisir une architecture qui permettra une modernisation de ces algorithmes d'encryptage en temps opportun. Il faudra donc établir un dialogue entre informaticiens, mathématiciens, physiciens et ... avocats!

La conduite des voitures autonomes au Québec : plusieurs questions demeurent

Par : **Léonie Gagné**

*avec la collaboration de
Élizabeth Martin-Chartrand,
étudiante en droit*

Selon une étude, 25 % des nouvelles voitures vendues dans l'ensemble du réseau mondial seront des voitures intelligentes dites autonomes d'ici 2035¹. Un groupe de recherche de l'université Princeton, aux États-Unis, évalue quant à lui que d'ici 2035-2050, plus de la moitié du parc automobile américain sera composé de ces automobiles autonomes².

Il existe présentement des voitures intelligentes sur le marché québécois, mais la conduite de voitures intelligentes dites autonomes aura sans aucun doute des répercussions sur plusieurs joueurs.

¹ Boston Consulting Group, (2016), *Autonomous Vehicle Adoption Study*.

² Jane Bierstedt et al., (2014), *Effects of Next-Generation Vehicles on Travel Demand and Highway Capacity*, FP Think Working Group.



Les voitures autonomes

Les voitures intelligentes utilisent les technologies de l'information et de la communication dans des systèmes préventifs d'accident présentant un niveau d'automatisation variable.

De manière simplifiée, l'automobile intelligente utilise un système de contrôle muni d'un algorithme qui prévoit comment l'automobile doit réagir. Ce système sophistiqué est connecté à des satellites et se maintient constamment à jour pour s'adapter aux nouvelles situations en enregistrant de nouveaux risques.

Il existe six niveaux d'automatisation pour les voitures³ :

- Niveau 0**, c'est-à-dire aucune automatisation;
- Niveau 1**, procurant des fonctions d'assistance au conducteur ;
- Niveau 2**, d'autonomie dite partielle, c'est-à-dire qui procure des fonctions d'assistance et d'accélération/décélération automatique, mais exige que le conducteur humain garde le contrôle sur toutes les fonctions de conduite dynamique ;
- Niveau 3**, c'est-à-dire d'automatisation conditionnelle, qui propose des fonctions de conduite dynamiques exécutées par le système de contrôle, mais nécessitant que le conducteur humain demeure disponible en tout temps ;
- Niveau 4**, c'est-à-dire d'automatisation importante, soit lorsque le système de contrôle d'un véhicule offre un contrôle total de toutes les fonctions de conduite, même en situation de sécurité critique ;
- Niveau 5**, d'automatisation complète, lorsqu'un véhicule exécute toutes les fonctions de conduite seul, sans possibilité pour l'humain d'intervenir

³ Pilot Project - Automated Vehicles, O Reg 306/15, art 2.

La Loi sur l'assurance automobile du Québec

La Loi sur l'assurance automobile du Québec (ci-après la « Loi ») prévoit un régime de responsabilité sans faute⁴. Ainsi, la Société de l'assurance automobile du Québec accorde des indemnités aux victimes d'accidents de voiture ayant subi un préjudice corporel sans égard à la responsabilité de quiconque. Selon la Loi, le propriétaire d'une voiture est toutefois responsable des dommages matériels causés par sa voiture et ne peut se décharger de cette responsabilité que s'il prouve la faute de la victime, celle d'un tiers ou la survenance d'un cas de force majeure. Or, il existe actuellement un flou juridique quant à la conduite des voitures autonomes au Québec, celle-ci n'étant à ce jour pas encadrée par la législation en vigueur.

En 2016, un premier projet pilote régissant la conduite de voitures autonomes au Canada a été présenté par le gouvernement ontarien. En plus de prévoir un investissement

sur les automobiles autonomes, ce projet a donné lieu à une modification au Code de la route⁵ ontarien en y incorporant le Règlement 306/15⁶. Bien que ce règlement autorise la conduite de voitures autonomes dans des situations précises, il n'a toutefois pas modifié le régime de responsabilité prévu à la loi ontarienne⁷.

Il semble nécessaire d'encadrer la conduite de voitures autonomes au Québec. D'une part, cette activité n'y est pas encore encadrée par la loi. D'autre part, la conduite de ces voitures suscite de nombreuses questions quant à la responsabilité en cas d'accident. En effet, la responsabilité à la suite d'un accident causé lors de la conduite d'une automobile autonome sera-t-elle celle du fabricant automobile ou demeurera-t-elle celle du conducteur? Qui assumera dorénavant ce risque?

⁴ Loi sur l'assurance automobile du Québec, R.L.R.Q. c. A-25, art 108 et ss.

⁵ Code de la route, L.R.O. 1990, c H.8.

⁶ Pilot Project - Automated Vehicles, O Reg 306/15

⁷ Loi sur les assurances, LRO 1990, c I.8, art. 267.1.

La responsabilité du fabricant au Québec

Au Québec, suivant le régime de la responsabilité du fabricant du Code civil du Québec⁸ et de la Loi sur la protection du consommateur⁹, une présomption existe à l'encontre du distributeur, du vendeur professionnel et du fabricant d'un bien lorsque l'acheteur de ce bien a établi que celui-ci a fait défaut ou s'est détérioré prématurément par rapport à un bien similaire, ce qui opère un déplacement du fardeau de preuve sur le fabricant.

Afin de repousser cette présomption, un fabricant ne peut plaider l'ignorance du défaut ni même l'usure du bien. Seulement deux moyens de défense s'offrent à lui¹⁰:

1. la démonstration de la faute de l'acheteur ou d'un tiers, ou de la survenance d'un cas de force majeure;
2. la preuve que l'état des connaissances scientifiques lors de la mise en marché du bien ne lui permettait pas de déceler un vice.

⁸ Code civil du Québec, R.L.R.Q. c. CCQ-1991, art. 1726 et ss.

⁹ Loi sur la protection du consommateur, R.L.R.Q. c. P-40.1, art 38.

¹⁰ ABB Inc. c. Domtar Inc., [2007] 3 RCS 461, par 72.

Commentaires

La question de savoir quand le transfert de responsabilité du conducteur d'un véhicule autonome vers le fabricant s'effectuera demeure nébuleuse pour l'instant. Il est toutefois à prévoir que le niveau de responsabilité du fabricant tendra à croître suivant l'accroissement du niveau d'utilisation de la technologie dans l'automatisation de la conduite d'un véhicule.

En effet, la conception même de certaines voitures autonomes fait en sorte qu'elles ne peuvent plus être contrôlées par l'humain : celui-ci devient donc simple passager, la conduite étant dorénavant entièrement assurée par le système de contrôle du véhicule. Ainsi, la

responsabilité entière lors d'un accident pourrait désormais reposer sur le fabricant de la voiture, mettant par le fait même en cause l'application du régime québécois de responsabilité du fabricant.

Si la responsabilité des fabricants de voitures autonomes devait être engagée en cas d'accident automobile, les recours pourraient mener à des litiges pyramidaux complexes. En effet, la responsabilité des souscontractants du fabricant d'une voiture autonome, tels le concepteur de l'algorithme de la voiture et l'entreprise responsable de la transmission de données, pourrait possiblement être engagée.

Le transfert de responsabilité vers les fabricants de voitures autonomes pourrait aussi avoir des répercussions en terme d'assurance. Tant la détermination des prestations d'assurance des conducteurs que des fabricants, que la souscription à des polices d'assurance par ces parties pourraient être affectées, le tout dépendant évidemment de qui sera appelé à assumer le risque.

La conduite de voitures autonomes pourrait également engendrer la venue de nouveaux joueurs en matière d'assurance automobile. Par exemple, Tesla propose présentement en Australie une police d'assurance adaptée à l'une de ses voitures intelligentes¹¹.

Conclusion

Les statistiques en termes de nombre d'accident démontrent que la conduite de véhicules autonomes engendrera une baisse d'accidents de la route, ceux-ci étant présentement attribuables aux États-Unis dans une proportion de 93 % à des erreurs humaines¹².

La conduite de voitures autonomes changera la manière dont nous effectuons nos déplacements et aura certainement aussi des incidences sur la législation québécoise en matière de responsabilité en cas d'accident d'automobile.

¹¹ Voir tesla.com

¹² John MADDUX, *Improving Driving Safety Through Automation*, Congressional Robotics Caucus, National Highway Traffic Safety Administration, 2012.

Nos experts des enjeux juridiques liés à l'intelligence artificielle



Eric Lavallée

Responsable du Laboratoire juridique Lavery sur l'intelligence artificielle (L³IA)



Guillaume Lavoie



Étienne Brassard



André Vautour



Jean-Sébastien Desroches



Laurent Bellemare-Proulx



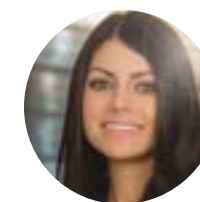
Léonie Gagné



Dave Bouchard



Shan Jiang



Katherine Athanasopoulos



Andrée-Anne Perras-Fortin

lavery
Avocats