Canadian Institute of Actuaries / Institut canadien des actuaires

Algorithmes fous

SAISAI ZHANG, *Ph. D., ASA*

Experte-conseil principale, actuariat, récompenses et analytique, Deloitte

Cet article fait partie de *Gestion du risque d'entreprise 2019 : La nouvelle vague de risques,* une collection d'articles portant sur la gestion du risque d'entreprise (GRE) de l'Institut canadien des actuaires (ICA). Lisez tous les articles à **cia-ica.ca/gre**.

Pourquoi devrions-nous porter attention au risque lié aux algorithmes?

Les algorithmes sont de plus en plus omniprésents dans notre quotidien. Avec les progrès de l'analytique des données, l'accélération de la puissance de traitement et les capacités grandissantes de l'informatique cognitive, le sens du terme « algorithme » s'est transformé, passant de programmes informatiques fondés sur des règles à des agents intelligents qui informent, voire prennent, des décisions d'une façon semblable au cerveau humain.

Ces décisions entraînent souvent des conséquences sociales ou sociétales, allant de la publicité ciblée et des offres de produits et de crédit à l'embauche, à la conduite automatisée et à la médecine personnalisée. Nous entrons dans une période où les algorithmes détiennent le pouvoir; et c'est pourquoi les retombées des algorithmes fous peuvent entraîner d'astronomiques pertes financières et atteintes réputationnelles.

Au cours de la dernière décennie, des défaillances très médiatisées d'algorithmes ont déjà fait les grands titres à l'échelle internationale. Le krach éclair de 2010, causé par la négociation par algorithme, a entraîné en quelques minutes une baisse de 9 % de l'indice industriel moyen du Dow Jones. Dans la période qui a précédé l'ouragan Irma en 2017, les algorithmes de gestion du rendement de Delta Airlines ont majoré les tarifs aériens à un niveau contraire à l'éthique dans une réaction automatisée à un choc de demande en état de crise. Tout récemment, on a soupçonné le Maneuvering Characteristics Augmentation System (un ensemble de capteurs et d'algorithmes) de l'appareil Boeing 737 Max d'être responsable de deux écrasements d'avion en 2018 et 2019, tuant au total 346 personnes à bord.

Alors pourquoi le risque lié aux algorithmes existe-t-il?

Les risques liés aux algorithmes peuvent provenir à chaque étape de la prise de décision automatisée ou semi-automatisée : de la saisie des données à la conception de l'algorithme et aux décisions résultantes. À mesure que nous délaissons les solutions fondées sur des règles pour adopter des solutions d'apprentissage automatique, les algorithmes commencent à se libérer des protocoles strictement programmés et à assimiler de nouvelles « règles » fondées sur des données.

Il en découle que ces algorithmes ne sont, au mieux, qu'aussi valables que les données qui les alimentent, lesquelles risquent d'être incomplètes ou superflues, ou inclure des biais sociétaux qui nécessitent une intervention humaine pour compenser les effets négatifs sur les résultats.

Par exemple, des recherches ont révélé qu'en 2015, les algorithmes de Google étaient beaucoup plus susceptibles de montrer des offres d'emplois très rémunérés aux hommes à la recherche d'emploi plutôt qu'aux femmes, laissant supposer que le sexe était un « facteur » ayant influencé les résultats de ses décisions. Bien que le sexe puisse très bien être un facteur prédictif valable d'après les données, le résultat accroissant l'écart salarial entre les sexes serait incompatible avec la mission et les valeurs de l'entreprise.

À l'instar de la modélisation statistique traditionnelle, la conception d'algorithmes d'apprentissage automatique est vulnérable à une variété de risques, comme des techniques, logiques ou hypothèses défectueuses de modélisation/étalonnage. Mais qui plus est, un ensemble unique de risques découle de leur opacité (c.-à-d. leur nature de « boîte noire »). Cette opacité se présente sous trois formes distinctes (Burrell, 2016) :

- La première est le secret d'entreprise intentionnel – si les entreprises adoptent des solutions exclusives, les rouages internes de leurs algorithmes sont considérés comme leurs secrets commerciaux et ne seraient pas apparents aux utilisateurs.
- La deuxième est l'analphabétisme technique – un algorithme peut être entièrement de source ouverte, mais il reste une « boîte noire » puisque le code de lecture et d'écriture constitue un ensemble de compétences spécialisées que seule la minorité possède.
- La troisième réside dans les caractéristiques des algorithmes combinées au volume nécessaire en vue d'une utilisation qui soit pertinente – cette forme d'opacité va au-delà de l'analphabétisme technique, car un technicien peut être en mesure de comprendre le code, mais être incapable de saisir comment les routines fonctionnent dans la réalité ou fournissent des conclusions dans un environnement de production réaliste, en raison de leur niveau élevé de complexité, de leur grand nombre de dimensions et de la complexité des liens entre de nombreuses sous-routines.

Le principal constat est que les entreprises doivent aspirer à comprendre pourquoi l'opacité existe et la placer dans le contexte où les algorithmes sont déployés, plutôt que de considérer l'opacité comme inévitable. Des stratégies ciblées de gestion des risques, comme l'audit des algorithmes ou leur validation, peuvent être élaborées pour atténuer efficacement les pertes éventuelles.

Les décisions provenant des algorithmes sont vulnérables au risque de mauvaise interprétation ou de mauvaise utilisation – ces risques sont particulièrement importants lorsque l'opacité est élevée. L'opacité entraîne également une multitude de risques issus de dilemmes éthiques, quand les algorithmes sont utilisés pour prendre des décisions à conséquences sociales qui ne peuvent être facilement expliquées aux personnes touchées.

Par exemple, les algorithmes de prédiction du cancer du sein peuvent améliorer le pouvoir prédictif de la disposition d'un point de vue mathématique, mais il se peut que les médecins spécialistes ne soient pas en mesure de déterminer pourquoi de telles indications de disposition existent, ce qui laisse le patient dans la position de faire d'importants choix de vie dans le noir.

La cybersécurité est également une préoccupation grandissante à l'ère moderne de la connectivité. Les entreprises doivent également être conscientes des risques liés à la sécurité des TI, car leur vulnérabilité au piratage peut avoir une incidence négative sur leurs données, leurs algorithmes et leurs résultats, pouvant les induire de force à de mauvaises conclusions.

Que pouvons-nous faire pour empêcher les algorithmes de produire des conséquences négatives?

Il est important de comprendre que l'engouement entourant l'« assurtech », ne peut que signifier que nous commençons à voir et à entendre davantage au sujet des algorithmes utilisés et intégrés à des solutions d'assurance modernes.

Il ne fait aucun doute que les algorithmes sont l'avenir pour augmenter l'efficience et la valeur. Alors que les sociétés d'assurance continuent d'examiner les cas d'utilisation d'algorithmes dans des domaines comme la tarification, l'analyse de la qualité des conducteurs, le traitement des réclamations, la détection de la fraude et l'analyse des sentiments des consommateurs, plusieurs questions urgentes doivent être prises en compte :

- Les entreprises sont-elles au courant de la présence de risques liés aux algorithmes?
- Comment les sociétés élaborent-elles des politiques et entretiennent-elles une culture d'entreprise qui garantit que les risques liés aux algorithmes sont compris dans l'ensemble de leurs fonctions?
- À quoi ressemble un cadre efficace de gestion du risque lié aux algorithmes?
- Quelles sont les considérations éthiques entourant la prise de décision automatisée, y compris la collecte de données et les préoccupations relatives au respect de la vie privée?
- Qui sont les talents appropriés à l'ère des algorithmes?
- Quelles nouvelles compétences les actuaires doivent-ils acquérir?
- Comment pouvons-nous conserver le plein contrôle des technologies qui ont une incidence sur nos vies et qui prennent des décisions pour nous?

Les organismes de réglementation pressent le pas en instaurant des mesures législatives réactives pour réglementer la prise de décisions issues d'algorithmes. Le Règlement général sur la protection des données (RGPD) de l'Union européenne (Union européenne, 2016), qui est entré en vigueur en 2018, impose des restrictions sur les algorithmes qui prennent des décisions fondées sur des données propres à un utilisateur, en insistant sur le « droit à l'explication » pour une personne qui fait l'objet d'une décision algorithmique qui l'affecte de façon significative. Qui plus est, il énonce explicitement qu'une personne a le droit de ne pas être assujettie à une décision fondée « uniquement » sur un traitement automatisé, y compris le profilage. En France, la loi pour une République numérique de 2016 impose au secteur public des règles plus strictes que le RGPD en étendant ce droit à des décisions simplement « appuyées » par un traitement algorithmique. Plus récemment, en 2019, les législateurs américains reconnaissent l'impact croissant des algorithmes sur les particuliers et ils insistent pour que les algorithmes soient testés afin de détecter les biais avant leur mise en production (Congrès américain, 2019).

Néanmoins, la réglementation sur la prise de décisions fondées sur des algorithmes est passablement à un stade précoce, et est principalement axée sur la transparence (c.-à-d. l'ouverture de la « boîte noire ») afin de promouvoir la responsabilisation. Bien que la transparence jette les bases d'évaluation de l'équité et de la probité, il manque encore un ensemble clair de normes pour établir une saine gestion des risques et pour s'assurer que les considérations d'ordre éthique sont au premier plan de la conception et du déploiement des algorithmes.

Les cabinets d'audit ont rapidement élargi leurs services pour y inclure des services de vérification et d'assurance des algorithmes. Ils jouent un rôle essentiel dans l'écosystème global de la gestion des risques liés aux algorithmes, car en fin de compte, l'audit des algorithmes exige une vaste expertise interdisciplinaire, y compris l'informatique, l'apprentissage statistique, l'éthique, le droit, le scepticisme professionnel et la communication. Les cabinets d'audit devront modifier leurs normes et lignes directrices en matière d'audit pour tenir compte du risque lié aux algorithmes, et mettre au point des moyens de mesurer la pertinence de la conception des algorithmes et des processus de prise de décisions. Les défis, comme les progrès technologiques rapides dans la conception d'algorithmes, l'évolution réglementaire, le sentiment des consommateurs, la confidentialité des données et les préoccupations en matière de cybersécurité, doivent être pris en compte et surveillés de près pour en assurer le succès.

L'avenir des algorithmes est déjà des nôtres, et les divers intervenants de notre écosystème canadien doivent jouer leur rôle pour être mieux informés de ses risques potentiels et exiger que les algorithmes soient déployés en toute sécurité à des fins commerciales et qu'ils soient examinés sous l'angle de la sécurité publique.

Sources

Burrell, J. « How the machine "thinks": Understanding opacity in machine learning algorithms », dans *Big Data & Society*, 2016, vol. 3, no 1, n.p. https://doi.org/10.1177/2053951715622512

Union européenne, Parlement et Conseil, *Règlement général sur la protection des données, Journal officiel de l'Union européenne*, L 119/1, le 4 mai 2016. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=OJ%3AL%3A2016%3A119%3ATOC

Congrès américain. *Algorithmic Accountability Act*, 2019. www.wyden.senate.gov/imo/media/doc/Algorithmic%20Accountability%20Act%20of%202019%20Bill%20Text.pdf