Canadian Institute of Actuaries / Institut canadien des actuaires

Algorithms gone wild

SAISAI ZHANG, *PhD, ASA*

Senior Consultant, Actuarial, Rewards and Analytics, Deloitte

This article is part of *Enterprise Risk Management 2019: The New Wave of Risks*, a collection of articles on enterprise risk management (ERM) from the Canadian Institute of Actuaries (CIA). The articles are written by subject matter experts, both actuaries and non-actuaries, giving us their own professional opinions and experiences, and highlighting new and emerging hot topics taking centre stage in today's world of risk management. **Read all the articles at cia-ica.ca/erm**.

Why should we care about algorithmic risk?

Algorithms are becoming increasingly ubiquitous in our day-to-day living. With the rise of advanced data analytics, faster processing power, and growing cognitive computing capabilities, the meaning of the term "algorithm" has gone through a transformative shift, from being rules-based computer programs to intelligent agents informing, or even making, decisions in ways similar to the human brain.

These decisions often give rise to social or societal consequences, ranging from targeted advertising and product and credit offers to hiring, automated driving, and personalized medicine. We are entering a time when algorithms rule, which is why the aftermath of "algorithms gone wild" can lead to astronomical financial and reputational losses.

In the past decade, high-profile algorithm failures have already made international headlines. The 2010 Flash Crash, caused by algorithmic trading, triggered a 9 per cent drop in the Dow Jones Industrial Average within minutes. In the initial lead-up to Hurricane Irma in 2017, the yield management algorithms of Delta Airlines raised airfares to an unethical extent as an automated response to a demand shock in the state of crisis. Most recently, the Maneuvering Characteristics Augmentation System (a set of sensors and algorithms) of the Boeing 737 Max aircraft was suspected to be the culprit of two plane crashes in 2018 and 2019, killing a total of 346 people onboard the flights.

So why does algorithmic risk exist?

Algorithmic risks can arise from each stage in the automated or semi-automated decision-making process: from data input to algorithm design and output decisions. As we move away from rules-based to machine-learning solutions, algorithms begin to break free of strictly coded protocols, and assimilate new "rules" based on data.

The implication is that these algorithms are, at best, only as good as the data feeding into them, which are at the risk of being incomplete or extraneous, or contain societal biases that require human intervention to counterbalance the negative impacts on the outcomes.

For example, research found that in 2015 Google's algorithms were much more likely to show advertisements of highly paid jobs to male job seekers than female

For example, research found that in 2015 Google's algorithms were much more likely to show advertisements of highly paid jobs to male job seekers than female, implying that gender was a "consideration" that drove its decision-making outcomes. Although gender may very well be a valid predictor according to data, the outcome of exacerbating the gender pay gap would be inconsistent with the company's mission and values.

Similar to classical statistical modelling, the design of machine learning algorithms is vulnerable to a variety of risks such as flawed modelling/calibration techniques, logic, or assumptions. But more importantly, a unique set of risks arise from their opacity (i.e., their "black box" nature). Such opacity comes in three distinct forms (Burrell 2016):

- The first is intentional corporate secrecy – if companies adopt proprietary solutions, the inner workings of its algorithms are considered to be its trade secrets and would not be visible to the users.
- The second is technical illiteracy – an algorithm may be completely open-source but remains a "black box" since reading and writing code (well) is a specialized skill set possessed only by the minority.
- The third resides in the characteristics of the algorithms together with the scale required for meaningful applications – this form of opacity goes beyond technical illiteracy, as a technician may be able to comprehend the code but unable to understand how the routines operate in action or give rise to conclusions in a realistic production environment, due to their high degree of complexity, high dimensionality, and the intricacy of inter-linkages among numerous subroutines.

The key takeaway is that companies should strive to understand why opacity exists, and situate it in the context where algorithms are deployed, rather than taking opacity as an inherent trait. Targeted risk management strategies, such as algorithm audit or validation, can be devised to effectively mitigate potential losses.

The decision outputs of algorithms are vulnerable to the risk of being misinterpreted or misused – such risks are especially prominent when opacity is high. Opacity also leads to a multitude of risks arising from ethical dilemmas, where algorithms are deployed on making socially consequential decisions

that cannot be easily explained to the affected individuals.

For example, breast cancer prediction algorithms may improve the predictive power of susceptibility from a mathematical point of view, but medical specialists may not be able to pinpoint why such indications of propensity exist, putting the patient in the position of making serious life choices in the dark.

Cyber security is also a growing concern in this modern age of connectivity. Companies should also be aware of IT security risks, as their susceptibility to being hacked can negatively affect their data, algorithms, and output, which would forcibly push them to arrive at flawed outcomes.

What can we do to prevent algorithms from producing negative consequences?

It is important to understand that with the buzz surrounding InsurTech, it can only mean that we are starting to see and hear more about algorithms being leveraged and integrated as part of modern insurance solutions.

There is no question that algorithms are the future for driving efficiency and value. As insurance companies continue to look into algorithmic use cases in areas such as pricing, driver performance analysis, claim processing, fraud detection, and consumer sentiment analysis, there are several pressing questions that need to be considered:

- Are companies aware of the presence of algorithmic risks?
- How do companies develop policies and cultivate a corporate culture that ensures algorithmic risks are understood across its functions?
- What does an effective algorithmic risk management framework look like?
- What are the ethical considerations surrounding automated decision making, including data collection and privacy concerns?
- Who are the right talents in the era of algorithms?
- What are the new skill sets actuaries need to acquire?
- How do we retain full control over the technologies that are impacting our lives and making the decisions for us?

Regulators are picking up their pace by introducing reactive legislative measures to regulate algorithmic decision making. The European Union's General Data Protection Regulation (GDPR) (EU 2016), which took effect in 2018, poses restrictions on algorithms that make decisions based on user-level inputs, stressing an individual's "right to explanation" when subjected to an algorithmic decision that significantly affects them. Most importantly, it explicitly states that an individual shall have the right not to be subject to a decision based "solely" on automated processing, including profiling.

Auditing firms will need to evolve their auditing standards and guidelines to capture algorithmic risk

The 2016 Digital Republic Act of France imposes stricter rules than the GDPR on the public sector by extending such a right to include decisions merely "supported" by algorithmic processing. More recently, in 2019 US lawmakers are recognizing the increasing impact of algorithms on individuals and are pushing for algorithms to be tested for biases before production (US Congress 2019).

Nonetheless, regulations on algorithmic decision making are largely at an early stage, focusing primarily on transparency (i.e., opening the "black box") in order to promote accountability. While transparency lays the groundwork for assessing fairness and probity, there still lacks a clear set of standards for establishing sound risk management, and for ensuring that ethical considerations are at the forefront of algorithm design and deployment.

Auditing firms have been quick to extend their services to include algorithm audit and assurance services. They play a vital role in the overall ecosystem of algorithmic risk management, as ultimately algorithm audit requires a multitude of interdisciplinary expertise, including computer science, statistical learning, ethics, legal, professional skepticism, and communication. Auditing firms will need to evolve their auditing standards and guidelines to capture algorithmic risk, and develop the means to measure the appropriateness of algorithm designs and decision-making processes. Challenges, such as rapid technological advancement in algorithm designs, regulatory movements, consumer sentiment, data privacy, and cyber security concerns, need to be considered and closely monitored to ensure success.

The future of algorithms is already here and the various stakeholders in our Canadian ecosystem need to play their part in order to become better educated on its potential risks, and demand that algorithms be safely deployed for commercial use and scrutinized with the lens of public security.

Sources

Burrell J. 2016. "How the machine "thinks": Understanding opacity in machine learning algorithms." *Big Data & Society* 3(1). https://doi.org/10.1177/2053951715622512

[EU] European Union, Parliament and Council. 2016. General Data Protection Regulation. *Official Journal of the European Union*, L 119/1. May 4. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=OJ%3AL%3A2016%3A119%3ATOC

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