lavery
Lawyers

Development of a legal definition of artificial intelligence: different countries, different approaches

March 10, 2020

Author

Eric Lavallée

Partner, Lawyer Partner, and Trademark Agent

As our society begins to embrace artificial intelligence, many governments are having to deal with public concern as well as the ongoing push to harness these technologies for the public good. The reflection is well underway in many countries, but with varying results.

The Office of the Privacy Commissioner of Canada is currently consulting with experts to make recommendations to Parliament, the purpose being to determine whether specific privacy rules should apply to artificial intelligence. In particular, should Canada adopt a set of rules similar to European rules (GDPR)? Another question raised in the process is the possibility of adopting measures similar to those proposed in the *Algorithmic Accountability Act of 2019* bill introduced to the U.S. Congress, which would give the U.S. Federal Trade Commission the power to force companies to assess risks related to discrimination and data security for AI systems. The *Commission d'accès à l'information du Québec* is also conducting similar consultations.

The Americans, in their approach, appear to also be working on securing their country's position in the AI market. On August 9, 2019, the National Institute of Standards and Technology (NIST) released a draft government action plan in response to a Presidential Executive Order. Entitled *U.S. LEADERSHIP IN AI: A Plan for Federal Engagement in Developing Technical Standards and Related Tools*[1], the plan calls for the development of new robust technologies to make AI solutions more reliable and standardized norms for such technologies.

Meanwhile, on November 21, 2019, the Congressional Research Service published an updated version of its report entitled *Artificial Intelligence and National Security*[2]. It presents a reflection on the military applications of artificial intelligence, and, in particular, on the fact that various combat devices have the capacity to carry out lethal attacks autonomously. It also looks at ways to counter deep fakes, specifically by developing technology to uncover what could become a means of disinformation. The idea is thus to bank on technological progress to thwart misused technology.

In Europe, further to consultations completed in May 2019, the Expert Group on Liability and New Technologies published a report for the European Commission entitled *Liability for Artificial Intelligence*[3], which looks into liability laws that apply to such technology. The group points out that, except for matters involving personal information (GDPR) and motor vehicles, the liability laws of member states aren't standardized throughout Europe. One of its recommendations is to standardize such liability laws. In its view, comparable risks should be covered by similar liability laws[4].

Earlier, in January 2019, the Consultative Committee of the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data published its *Guidelines on Artificial Intelligence and Data Protection*[5],whichincludes recommendations to comply with human rights conventions not only for lawmakers, but for developers, manufacturers and service providers using such technology as well.

Even with these different approaches, one fundamental question remains: If special rules are to be adopted, to which technologies should they be applied? This is one of the main questions that the Office of the Privacy Commissioner of Canada is posing.

In other words, what is artificial intelligence? The term is not clearly defined from a technological standpoint. It covers a multitude of technologies with diverse characteristics and operating modes.

This is the first issue that lawmakers will have to address if they wish to develop a legal framework specific to AI.

The document of the European expert group mentioned above gives us some points to consider that we believe to be relevant. In the group's view, when qualifying a technology, the following factors should be taken into consideration:

Its complexity;
Its opacity;
Its openness to interaction with other technologies;
Its degree of autonomy;
The predictability of its results;
The degree to which it is data-driven;
Its vulnerability to cyber attacks and risks.

These factors help to identify, on a case-by-case basis, the risks inherent to different technologies.

In general, we think it preferable to not adopt a rigid set of standards that apply to all technologies. We rather suggest identifying legislative goals in terms of characteristics that may be found in many different technologies. For example, some deep learning technologies use personal information, while others require little or no such information. They can, in some cases, make decisions on their own, while in others, they will only help to do so. Finally, some technologies are relatively transparent and others more opaque, due in part to technological or commercial constraints.

For developers, it becomes important to properly label a potential technology in order to measure the risks its commercialization involves. More specifically, it may be important to consult with legal experts from different backgrounds to ensure that the technology in question isn't completely incompatible with applicable laws or soon to be adopted ones in the various jurisdictions where it is to be rolled out.

---

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. Ibid, p. 36.

5. https://rm.coe.int/guidelines-on-artificial-intelligence-and-data-protection/168091f9d8