

# OVERVIEW OF THE CANADIAN LEGAL FRAMEWORK RELATIVE TO ARTIFICIAL INTELLIGENCE SYSTEMS FOLLOWING THE ADOPTION OF THE AI ACT IN EUROPE

Posted on August 9, 2024

**Categories:** [Insights](#), [Publications](#)

Artificial intelligence (“**AI**”) software, tools, products, and services are now an integral part of our lives, whether we are conscious of it or not. When we shop online, transact with businesses in person, navigate the web, or use mobile applications, organizations may leverage AI systems to engage with us, learn about our preferences and habits, and attempt to develop data-driven business intelligence to achieve their ends. As the AI technology continues to evolve, it brings both unprecedented opportunities and risks.

On August 1, 2024, the European Union’s *Regulation Laying Down Harmonised Rules on Artificial Intelligence* (“**AI Act**”) came into force, setting out a comprehensive set of rules and obligations relative to AI systems. As Canadian organizations assess their obligations under the AI Act, it is a good opportunity for us to provide you with an overview of the Canadian legal framework applicable to AI systems so you can implement a comprehensive compliance strategy.

In this article, we’ll begin by providing you with a general bird’s-eye view of the AI Act, followed by a more detailed view of the Canadian legal framework applicable to AI systems.

## **A. Overview of the European AI Act**

To start with, it’s important to bear in mind that our overview of the AI Act here is intended to provide you with general information only. Should you need legal advice with respect to the AI Act, please consult with a qualified attorney.

With that said, let’s begin.

### **1. What is the purpose of the AI Act?**

The main reason why the European Union adopted the AI Act is to balance innovation with appropriate safeguards. In fact, the AI Act specifically prohibits certain types of AI practices and tightly regulates AI systems classified as “high-risk.” Limited-risk or low-risk AI systems may also be impacted but not as rigorously as high-

risk AI systems.

## **2. What is an “AI system” under the European AI Act?**

Based on the simple reading of the European AI Act, “artificial intelligence systems” is defined as: (i) any software that is developed with one or more of the techniques and approaches identified in the Act (such as machine learning, logic-based or knowledge-based, or statistical approaches), and (ii) software that can generate outputs such as content, predictions, recommendations, or decisions influencing the environments with which they interact.

## **3. To whom does the AI Act apply?**

It appears that the AI Act may apply to: (i) providers placing AI systems on the market or putting them into service in the European Union (“EU”) (whether or not such providers have an establishment within the EU); (ii) users of AI systems located in the EU; and (iii) providers or users of AI systems located outside of the EU but where the output produced by the AI system is used in the EU.

## **4. What are the prohibited AI practices?**

The AI Act prohibits certain types of AI practices altogether. For example: (i) AI systems deploying subliminal techniques beyond a person’s consciousness causing them harm; (ii) AI systems that exploit a person or a group of persons’ vulnerabilities causing them harm; or (iii) a public authority’s use of AI systems with social scoring leading to detrimental outcomes for individuals.

## **5. What are “High-risk” AI systems?**

Based on our simple reading, it appears that the AI Act establishes a method for the classification of high-risk AI systems. AI systems will be classified as high-risk to the extent that they pose significant risks to health, safety, or fundamental rights. For example, this can include AI systems used as a safety component of a product, for biometric identification and categorization of individuals, for recruitment purposes, and various other types of AI systems.

Following this brief overview of the AI Act, let us move on to a more detailed overview of the Canadian legal framework relative to AI systems.

## **B. Overview of the Canadian Legal Framework Relative to Artificial Intelligence Systems**

### **1. Does Canada have a comprehensive legal framework relative to artificial intelligence similar to the AI Act?**

As of the writing of this article, Canada does not have comprehensive legislation governing AI systems similar

to the European AI Act. As such, organizations must consider a patchwork of different laws and regulations at the federal and provincial levels to ensure that they design, develop, deploy, distribute, and sell their AI systems within the bounds of Canadian laws.

## **2. Will Canada adopt a comprehensive legal framework relative to artificial intelligence systems?**

Recognizing the rapid evolution of AI technologies and the potential risk of harm to Canadians, in 2022, the Canadian federal government tabled [Bill C-27](#) aimed at modernizing the Canadian privacy statute and introducing the *Artificial Intelligence and Data Act* ("**AIDA**") setting out a legal framework specifically applicable to AI systems. The objective of the AIDA is to ensure that organizations have the proper legal foundations for the responsible design, development, and deployment of AI systems in Canada. At this time, Bill C-27 remains before the House of Commons and is going through the Canadian legislative process.

## **3. What does the AIDA entail?**

The main objective pursued by the Canadian government with AIDA is to ensure that AI systems are designed, developed, and deployed in a safe manner for the benefit of society and without harm to Canadians. In addition, the government's objective is to hold organizations involved in the design, development, and deployment of AI systems accountable for the products and services they put in the Canadian market or enable Canadians to use.

AIDA uses a principles-based approach requiring providers of high-impact systems to make sure their AI systems are carefully assessed for potential risk of harm or bias, adequately inform users as to the AI system's intended uses and limitations and adopt risk mitigation measures on a continual basis.

### **a. What is an "Artificial Intelligence System" under AIDA?**

Based on the current draft of Bill C-27, AIDA defines an "artificial intelligence system" as "a technological system that, autonomously or partly autonomously, processes data related to human activities through the use of a genetic algorithm, a neural network, machine learning or another technique in order to generate content or make decisions, recommendations or predictions." To the extent that your software, application, or tool satisfies such requirements, it will be considered an "AI system" under AIDA.

### **b. To whom will AIDA apply?**

Based on the current draft of Bill C-27, AIDA applies to any organization, including a trust, a joint venture, a partnership, an unincorporated association, or any other entity that, in the course of international or interprovincial trade and commerce, designs, develops or makes available for use AI systems or manages its operation. As such, AIDA can possibly target a broad range of organizations and actors in the AI space,

including developers, providers, operators, or others.

### **c. What are “high-impact systems” under AIDA?**

Based on the current draft of Bill C-27, AIDA defines “high-impact systems” as artificial intelligence systems that meet certain criteria set out by regulation. As such, we do not currently have a concrete definition of high-impact systems and will not until a regulation is adopted to this effect, should Bill C-27 be adopted as currently drafted. The Canadian government considers it more appropriate to define “high-impact systems” in a subsequent regulation for better precision in the identification of such systems, to ensure better interoperability with other international frameworks governing AI systems, and to ensure that advancements in technology are better tracked in law.

In [\*The Artificial Intelligence and Data Act \(AIDA\) – Companion\*](#) document, the government of Canada identifies certain key factors that may need to be considered in defining high-impact systems for the purposes of adopting a regulation, namely:

- “Evidence of risks of harm to health and safety, or a risk of adverse impact on human rights, based on both the intended purpose and potential unintended consequences;
- The severity of potential harms;
- The scale of use;
- The nature of harms or adverse impacts that have already taken place;
- The extent to which for practical or legal reasons it is not reasonably possible to opt-out from that system;
- Imbalances of economic or social circumstances, or age of impacted persons; and
- The degree to which the risks are adequately regulated under another law”.

## **4. In the absence of a comprehensive law in Canada, how are AI systems regulated?**

As mentioned above, organizations should be mindful of the application of a variety of statutes and regulations applicable to their design, development, and deployment of AI systems in Canada. Here is a brief summary of the current legal landscape relative to AI systems (keeping in mind that this does not represent an exhaustive overview).

### **a. The Application of Privacy laws**

Organizations may be subject to federal or provincial privacy laws if their AI systems collect, use, process, store, or otherwise handle personal information. For example, AI systems scraping data online, including personal information, will need to comply with Canadian or provincial privacy laws for having collected, processed, and used such personal information.

The [\*Personal Information Protection and Electronic Documents Act\*](#) ("**PIPEDA**") is a federal statute that may apply to organizations. You can also have provincial privacy statutes deemed substantially similar to PIPEDA that may apply instead of PIPEDA, particularly in British Columbia, Alberta, and Quebec.

On December 7, 2023, the Office of the Privacy Commissioner of Canada ("**OPC**"), along with provincial privacy authorities, published the [\*Principles for responsible, trustworthy and privacy-protective generative AI technologies\*](#) ("**Generative AI Guidance**") to help organizations developing, providing, or using generative AI technologies comply with the privacy laws and regulations in Canada. The OPC is of the view that "while generative AI tools may pose novel risks to privacy and raise new questions and concerns about the collection, use and disclosure of personal information, they do not occupy a space outside of current legislative frameworks."

With the Generative AI Guidance, the OPC identifies the considerations for the application of the key privacy principles to generative AI technologies, enabling providers, developers, and organizations using generative AI to comply with their respective privacy obligations within the current parameters of the law.

#### **b. The Application of Employment Laws**

There are various provincial laws setting out each province's minimum employment standards. Although such laws are not specifically designed to govern AI systems, employers are cautioned to use their AI systems within the bounds of such minimum employment standards to avoid unintended violations. For example, a company using an AI system to monitor employee performance may violate applicable labour laws if the AI model unfairly penalizes employees with various disabilities.

#### **c. The Application of Human Rights Laws**

In Canada, the [\*Canadian Human Rights Act\*](#) prohibits discrimination on various grounds such as race, national or ethnic origin, colour, religion, age, sex, sexual orientation, gender identity or expression, marital status, family status, genetic characteristics, disability or conviction for an offence for which a pardon has been granted or in respect of which a record suspension has been ordered. Provincial human rights legislation may also find application, for instance, the *Charter of Human Rights and Freedoms* in Quebec or the *Human Rights Code* in Ontario.

As such, organizations may be exposed to liability under Canadian human rights statutes to the extent they use AI systems that result in discriminatory outcomes. For example, an employer using an AI system (containing biases) to screen job applications may inadvertently discriminate against certain groups of applicants.

#### **d. The Application of Intellectual Property Laws**



From an intellectual property perspective, although the laws do not specifically address AI systems, they do present the framework within which intellectual property, such as patents, copyrights, trademarks, and other intellectual property rights, may be protected. For example, the [Copyright Act](#) can be used to protect AI systems, such as the software or databases they may contain, among other things.

What about the protection of works produced by generative AI systems? Could copyright protection be granted to an AI system as its “author”? Could an AI system be considered an “inventor” for patent purposes? Currently, there are some debates on this topic. For instance, in the [Consultation paper: Consultation on Copyright in the Age of Generative Artificial Intelligence](#), the federal government states that the “rapid developments in AI technology, combined with its burgeoning application across various sectors of the economy, lead the Government to consider whether the [Copyright] Act is suited to address questions of authorship and ownership of AI-generated works or AI-assisted works.” The government further states “there could be ways of clarifying first ownership of AI-generated or AI-assisted works by reconsidering how to define an author, or even without relying on authorship”.

There may also be a risk for AI systems to infringe on the intellectual property rights of others. For example, the employees of a company may use generative AI systems to create an image that may potentially infringe the copyrights of an artist.

Organizations should carefully assess their rights and obligations under Canadian intellectual property laws to ensure their AI systems are well protected and do not infringe on third-party intellectual property rights.

#### **e. The Application of Consumer Protection Laws**

Organizations should be cautious in ensuring that their AI systems are offered to consumers in compliance with any applicable provincial consumer protection statute. In addition to the application of general consumer protection laws in each province, certain specific statutes may also apply governing consumer-related activities, such as the [Canada Consumer Product Safety Act](#), the [Food and Drugs Act](#), or the [Motor Vehicle Safety Act](#), among others, that may also apply.

For example, a company may violate consumer protection laws if it makes AI systems available to consumers without the proper consumer disclosures, does not respect the consumer contract formation formalities, makes it difficult or impossible for consumers to cancel their contracts, or charges hidden fees, among other things.

#### **f. Criminal Code**

To the extent that a person uses AI systems to commit a crime, the [Canadian Criminal Code](#) may apply. For example, a person may use AI systems to impersonate another to commit a crime, to commit acts of fraud,

cybercrime, or identity theft, or to engage in any other activity or conduct using or facilitated by AI systems that may be considered criminal conduct. As such, although the *Criminal Code* is not designed to directly regulate AI systems, nefarious uses of AI systems can lead to criminal investigations by the authorities and possibly prosecution.

## **Conclusion**

Canadian and the European Union authorities recognize the need to establish a legal framework governing AI systems promoting innovation and benefiting society in a fair, transparent, and safe manner.

With the adoption of the AI Act, the European Union now has a comprehensive piece of legislation setting out measures for the responsible and transparent use of AI. In Canada, AI systems must be used within the parameters of current laws and regulations, such as privacy laws, consumer protection laws, human rights laws, or others, depending on the nature of a company's activities or use of the AI system.

However, if Bill C-27 is adopted, Canada will also have a comprehensive statute specifically designed to regulate AI systems. As at the writing of this article, the adoption of Bill C-27 remains speculative.

In the end, what is reassuring is that Canada and the European Union are working to achieve the same objective: the responsible design, development, and deployment of AI systems.

by [Amir Kashdaran](#)

## **A Cautionary Note**

The foregoing provides only an overview and does not constitute legal advice. Readers are cautioned against making any decisions based on this material alone. Rather, specific legal advice should be obtained.

© McMillan LLP 2024