Artificial Intelligence Regulation in Canada: Breakdown for Businesses

Description

On June 16, 2022, the federal government introduced Bill C-27, the *Digital Charter Implementation Act, 2022*. This Bill includes three separate pieces of legislation aimed at overhauling Canada's private sector federal privacy laws:

1. 1. The *Consumer Privacy Protection Act* ("CPPA");
2. 2. The *Personal Information and Data Protection Tribunal Act* ("PIDPTA"); and
3. 3. The *Artificial Intelligence and Data Act* ("AIDA" or the "Act").

The AIDA regulates artificial intelligence, defined broadly (see below), but the CPPA also includes the regulation of automated decision systems. The CPPA defines those systems as technology that assists or replaces the judgment of human decision-makers through the use of a rules-based system, regression analysis, predictive analytics, machine learning, deep learning, a neural network or other technique (CPPA, s 2). This definition includes artificial intelligence systems ("AI Systems") as defined in the AIDA, but the focus of each legislation is distinct. The CPPA has a more micro focus, being concerned with the accuracy of decisions rendered using personal information and providing individuals with the right to request an explanation of how a prediction, recommendation or decision having a significant impact on them was made. The AIDA, on the other hand, is more macro focused, aimed at regulating processes that can lead to broader, societal level risks associated with the use of AI Systems, such as human rights infringements. An article regarding an overview of the CPPA is forthcoming. In this article, we will focus on the AIDA.

Introduction

The AIDA, if passed as drafted, takes a principled approach, rather than a rights-based approach. It is intended to regulate international and interprovincial trade and commerce in AI Systems by establishing common requirements and prohibiting certain conduct. The AIDA does not introduce any new consumer rights, but it does introduce the role of Artificial Intelligence and Data Commissioner (the "Commissioner"). The Minister can designate a senior official in their department to fill the role of the Commissioner, and delegate any power, duty or function on them (except making regulations).

AI System is defined broadly and means "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" (AIDA, s 2).

The AIDA imposes obligations on all the actors involved in AI Systems and their use from those who provide the data used to train the system, to designers, developers, and providers, to those who manage their operation. The Act defines "Regulated Activity" as any of the following activities carried out in the course of international or interprovincial trade and commerce:

- Processing or making available for use any data relating to human activities for the purpose of

designing, developing or using an AI System; or

- Designing, developing or making available for use an AI System, or managing its operations (AIDA, s 5(1)).

The AIDA also states that a person is responsible for an AI System if, in the course of international or interprovincial trade and commerce, they design, develop, or make available for use the AI System or if they manage its operation. This definition could introduce interesting implications for licenses that we will discuss below.

Obligations

The primary obligations imposed by the AIDA are included in sections 6 to 12. The Act imposes obligations with respect to anonymized data, AI Systems generally, and with respect to "high-impact" AI Systems. While we have a lot to digest in this Act, much of the details of the obligations imposed have yet to be revealed. Many of the provisions in the AIDA specify that the obligation must be done "in accordance with the regulations", which have yet to be provided. The Act imposes additional obligations on persons responsible for high-impact AI systems, but the definition of "high-impact system" refers to criteria established in the regulations. Acknowledging this gap in our current knowledge, what follows is an outline of what we know, and what we do not know because it will be established by regulations.

Anonymized Data

If you carry out a regulated activity and process or make available anonymized data in the course of that activity, you have to establish measures with respect to the manner in which the data is anonymized and how it is used and managed (AIDA, s 6); however, these measures must be established "in accordance with the regulations." We can therefore look forward to further guidance with respect to these measures in the form of regulations not yet available.

Assessments

Anyone responsible for an AI System must conduct an assessment to determine whether the system is "high-impact" (AIDA, s 7); however, the criteria to be used to conduct this assessment are to be provided in the regulations, which are not yet available.

High-Impact Systems

If it turns out you are responsible for a high-impact system, additional obligations are imposed, including:

- establishing measures to identify, assess, and mitigate risks of harm or biased output (which are defined terms) that could result from the use of the system (AIDA, s 8);
- establishing measures to monitor compliance with those mitigation measures, and their effectiveness (AIDA, s 9);
- publishing plain-language explanations of the AI System (AIDA, s 11); and
- notifying the Minister if the use of a high-impact system results or is likely to result in material

harm (AIDA, s 12).

Biased output means content that is generated, or a decision, recommendation or prediction that is made, by an AI system and that adversely differentiates, directly or indirectly and without justification, in relation to an individual on one or more of the prohibited grounds of discrimination in section 3 of the *Canadian Human Rights Act*. It excludes such content where the purpose and effect are to prevent, eliminate or reduce disadvantages suffered by any group of individuals when those disadvantages would be based on or related to the prohibited grounds. What is not clear yet is what does and does not constitute "justification" in this definition, as this has been left to regulations to define.

Harm means physical or psychological harm to an individual, damage to an individual's property, or economic loss to an individual. However, what constitutes "material harm" for the purposes of notifying the Minister is the subject of regulation.

Persons who make a high-impact system available for use must publish a plain-language explanation of

- how the system is intended to be used;
- the types of content it is intended to generate and the decisions, recommendations or predictions it is intended to make;
- the mitigation measure established under s 8; and
- any other information prescribed by regulation.

Persons who manage the operation of a high-impact system must publish a plain-language explanation of

- how the system is used;
- the types of content it generates and the decisions, recommendations or predictions it makes;
- the mitigation measures established under s 8; and
- any other information prescribed by regulation.

The regulations may outline the time and manner of these plain-language summaries, as well as any additional information required.

The definition of a person responsible for an AI System in conjunction with these obligations may operate to change the nature of ongoing relationships between those who develop, design and provide AI Systems for use (the "Licensors") and the customers that use such systems (the "Licensees"). The Licensors may have continued obligations with respect to their AI Systems that necessitate increased auditing powers in their license agreements to ensure they are capable of meeting their obligations under the Act. Licensees may need to prepare themselves for invasions into their operations that they would not previously have expected, and pay even closer attention to confidentiality clauses in those license agreements.

Record Keeping

Persons carrying out a regulated activity must keep records describing the reasons supporting their analysis of whether the AI System they are responsible for is high-impact, as well as documenting the measures they are required to establish relating to anonymized data, risk assessment and mitigation, and monitoring compliance with and effectiveness of those measures.

Compliance and Enforcement

The AIDA provides the Minister (or the Commissioner, if the powers are delegated) with broad powers to require by order any of the following:

- Production of the records relating to the required measures at any time;
- Production of the records relating to the high-impact assessment where there are reasonable grounds to believe a high-impact system could result in harm or biased output;
- Where there are reasonable grounds to believe there has been a contravention of the Act or any of the Minister's orders, the Minister can require a person to conduct an audit or engage an independent auditor at their own cost to provide a report to the Minister;
- Requiring the subject of the audit to implement measures to address anything referred to in the audit;
- Where there are reasonable grounds to believe the use of a high-impact system gives rise to serious risk of imminent harm, the Minister can require that the person responsible cease using or providing the high-impact system; and
- Require persons responsible to publish information, including information relating to the audit.

The Minister also has the power to make certain publications themselves. The Minister has the power to "name and shame" by publishing information about contraventions of the AIDA in order to encourage compliance, where it is in the public interest to do so. The Minister can also publish information about an AI System without the knowledge or consent of the person responsible for it, if there are reasonable grounds to believe the use of such a system gives rise to a serious risk of imminent harm and publication is essential to prevent that harm.

The AIDA utilizes administrative monetary penalties ("AMPs") and offences. AMPs are available for anyone found to have committed a violation of the Act; however, no further details are provided at this point. The regulations will outline the sections that would result in a violation if contravened, the amount or range of amounts that may be imposed, and the factors to be taken into account when imposing an AMP. There is nothing to suggest that the Minister or Commissioner would not be responsible for imposing the AMPs.

The offences can be prosecuted as summary conviction offences (less serious) or indictable offences (more serious), and have varying penalties depending on the offence. Contravening sections 6 to 12 of the Act or obstructing the Minister, their delegate, or an independent auditor can result in penalties ranging from the greater of $5,000,000 and 2% of gross global revenue in the financial year preceding sentencing ("GGR") to the greater of $10,000,000 and 3% of GGR. Organizations are vicariously liable for the actions of their employees and agents unless they can establish the offence was committed without the knowledge and consent of the accused. Establishing due diligence to prevent the conduct of the offence can be a complete defence.

Other offences include:

- Possessing or using personal information while knowing or believing it was obtained or derived, directly or indirectly, as a result of the commission of an offence under federal or provincial legislation, whether that act was committed in Canada or elsewhere;
- Without lawful excuse and knowing or being reckless as to whether the use of an AI System is likely to cause serious physical or psychological harm to an individual or substantial damage to the individual's property, making an AI System available for use and the use causes such harm or damage; and
- With the intent to defraud the public and cause substantial economic loss to an individual, making an AI System available for use and the use causes that loss.

These offences can result in penalties ranging from fines of not more than the greater of $20,000,000 and 4% of GGR to $25,000,000 and 5% of GGR for organizations convicted. Where the accused is an individual, punishment can range from a fine of not more than $100,000 and/or imprisonment of two years less a day to a fine in the discretion of the court and/or imprisonment of up to five years less a day.

Conclusion

There is an ongoing trend towards harmonizing privacy and data protection laws across jurisdictions, and artificial intelligence has become a hot topic. The European Union has introduced a draft Artificial Intelligence Act. The Federal Trade Commission in the U.S. has indicated its focus on AI Systems, and even recently required that an organization delete algorithmic data obtained illegally and destroy the associated algorithms. As well, the draft bipartisan federal privacy legislation recently introduced in the U.S. includes some regulation of AI Systems. Clearly, regulation of artificial intelligence is not going away. While the AIDA may not be passed exactly as currently written, it is very likely some version of it will be passed.

Although there will certainly be a transition period once the law is enacted, in whatever final form it takes, businesses should be ready to amend their operations when that happens. Stay tuned for updates as the bill moves through the process of becoming law.