A turning point for AI in Canada in 2026?

March 25, 2026

In this article, we take a step back to reflect on the developments that shaped the recent AI landscape in Canada and highlight the emerging trends organizations should focus on in 2026.

Grouped under overarching themes, BLG lawyers selected the most important insights from the past year to offer a clear overview of what to anticipate for this year along with actionable takeaways. This complements BLG's *2025 Privacy and Cybersecurity Year in Review*, as well as our recently updated *Guide on Québec's Private Sector Act*.

Key takeaways

- The past year underscored that, on the one hand, new AI-related risks are emerging and existing ones are amplified, while on the other, regulatory scrutiny is heightened. Organizations are encouraged to reinforce their governance and supervision frameworks to keep pace with evolving regulatory expectations.
- Organizations should strengthen enterprise-wide AI governance programs grounded in algorithmic and impact assessments, human-in-the-loop safeguards, and rigorous vendor due diligence. This includes ensuring that all AI use complies with existing privacy and cybersecurity obligations, particularly for the use of agentic AI.
- Where necessary, these frameworks should be tailored to different uses of AI tools and to different positions within organizations.
- In the absence of AI-specific legislation, soft-law standards and sector-specific guidance will continue to serve as critical benchmarks.
- Organizations that invest early in robust governance and supervision frameworks will be best positioned to innovate responsibly while maintaining compliance and public trust.

National AI strategy: Anticipated updates in 2026

The year 2025 was pivotal for the development of the Pan-Canadian Artificial Intelligence Strategy.

A major development was the creation of an AI Strategy Task Force, which invited input from the industry, academia, and the public to shape the next phase of Canada's AI

roadmap. In late February, the Government published a report summarizing the answers received from the public and the Task Force. Over 11,000 participants submitted answers.

Namely, respondents highlighted the importance of accelerating AI adoption across the economy while ensuring appropriate safeguards, governance, and risk management, such as with certification standards and independent audits. With the feedback received, the federal government has indicated that a revised AI strategy is to be expected this year.

Through Budget 2025, Canada established AI as a central pillar of the federal economic strategy. This includes substantial investments in sovereign compute capacity and the expansion of AI adoption across the public sector. Collectively, these measures point to a coordinated and ambitious national direction. Yet, Canada still finds itself without a federal AI statute after the Artificial Intelligence and Data Act (AIDA) died on order paper as part of Bill C-27 in January 2025.

In 2026, a successor to the now-defunct AIDA is widely expected to be tabled. While no official statement has been released on the potential bill, Minister of Artificial Intelligence and Digital Innovation Evan Solomon announced his intention to propose a law that would not be a repeat of AIDA but instead be its own regulatory initiative. Together, these developments position the coming year as a significant moment for AI as a national priority.

What does this mean for organizations?

For organizations, these developments underscore the need for proactive compliance and risk-management measures. Businesses are encouraged to continuously assess their AI activities against existing legal obligations and evaluate whether appropriate resources can be mobilized to adapt to future changes.

As we progress into the year, organizations should closely monitor upcoming legislative and policy updates. Rest assured that BLG will deliver timely commentary on the matter.

Responsible AI adoption: A key priority across sectors

As organizations across sectors transition from pilot projects to enterprise-wide AI deployment, Canadian regulators focused on promoting responsible adoption in 2025. Regulatory bodies increasingly recognized that scaling AI brings not only opportunities but amplified risks in the operational, ethical, and consumer protection spheres.

In the financial sector

Regulators identified these risks and put forth guidance on how to manage them. The Office of the Superintendent of Financial Institutions (OSFI) released updated expectations under Guideline E-23 – Model Risk Management, explicitly expanding its

scope to encompass AI and machine-learning-based systems used by federally regulated financial institutions.

The guideline introduces strengthened enterprise-wide controls, expectations for proportional governance, and clearer accountability for third-party AI models, reflecting OSFI's concern that rapid AI integration could exacerbate model risk if left unmanaged.

In parallel, the Financial Consumer Agency of Canada (FCAC) hosted four workshops as part of the Financial Industry Forum on Artificial Intelligence with industry leaders to highlight best practices that should be followed to respect principles of fairness, accuracy, and transparency.

Meanwhile in Québec, the Autorité des marchés financiers (AMF) published guidance (available in French only) which identifies expectations that financial institutions should aim to meet over the lifecycle of the AI system, such as data sourcing and oversight measures. Moreover, the document targets specific governance principles that apply to boards and executives and should be implemented within institutions. Altogether, these guidance documents are further contributing to a converging national emphasis on trustworthy AI practices.

In the healthcare sector

Privacy regulators are focussing on challenges arising from the use of AI scribes. After a confidentiality incident involving the use of an AI scribe in a hospital setting occurred, both Ontario and British Columbia's privacy commissioners issued detailed guidance for healthcare providers identifying best practices both to comply with privacy requirements and to use the tool responsibly.

The new guidance highlights the need for a privacy-by-design approach, rigorous vendor oversight, and mandatory human oversight of AI-generated clinical documentation, especially given the severity of potential consequences for patients in case of a breach or inaccuracy.

In the absence of AI-specific legislation at the federal or provincial level, these guidelines add to the body of soft law standards that have become influential benchmarks for organizations. Looking ahead, in 2026 the expansion of AI use cases will only continue to accelerate, along with the risks that come with such technology.

How can organizations adopt AI responsibly?

Organizations need to operationalize responsible AI practices now, rather than treating them as mere advice. Businesses deploying AI systems should embed privacy-by-design, data governance, and human-oversight measures throughout the AI lifecycle, from data sourcing and model development to deployment and monitoring.

These governance principles should apply at different levels within the organization, with boards and senior management maintaining visibility over AI-related risks. Otherwise, businesses may face regulatory scrutiny, operational disruption, and reputational harm.

For more information:

- OSFI responds to the growing use of AI: Key updates to guideline E-23 (Nov. 2025)
- Québec's Autorité des marchés financiers moves on AI oversight for financial institutions, including insurers (July 2025)
- Fear not the black box: How responsible AI adoption can drive innovation and productivity (Feb. 2025)

AI training and privacy: Regulatory scrutiny intensifies

OPC investigates the usage of personal data to create deepfakes

A key development in 2025 was the Office of the Privacy Commissioner of Canada (OPC) launching an ongoing investigation into X Corp.'s use of AI, examining whether X is collecting, using, and disclosing Canadians' personal information without valid and meaningful consent, particularly for training its AI models.

Recently, the OPC expanded this investigation following multiple reports that Grok had been used to generate non-consensual sexualized deepfake images of real individuals.

The OPC's approach echoes its earlier joint investigation into OpenAI, which also focused on issues of consent, transparency, and purpose limitation. These investigations highlight that when it comes to AI training, privacy concerns are under scrutiny by regulators. Until official findings are issued, organizations should tread lightly when considering training AI models or that of third-party vendors with customer data.

Clearview AI findings reveal that not all online information can be used without consent

On the question of using information available online for AI training, 2025 also brought the notable *Clearview AI v. Alberta decision*. While the Court emphasized that not all online information automatically qualifies as "publicly available" and therefore exempt from consent requirements, it ultimately deemed the exception as unconstitutional, finding that its narrow definition of "publicly available information" unduly restricted freedom of expression.

Clearview AI v. Alberta thus raises complex questions about the permissible use of publicly accessible data for AI training, which remain unsettled until the province's legislator officially amends the law.

Moreover, as well as the Alberta decision, British Columbia's ruling on Clearview AI also confirms that foreign entities who have no assets physically present in the country can still be subject to Canadian privacy laws.

The test is whether there is a sufficiently real link between the foreign entity and the jurisdiction, such as collecting personal information of individuals who are on the given

territory. Non-Canadian organizations are therefore not automatically exempt from the application of provincial laws.

The Court of Appeal in British Columbia recently confirmed these findings, thereby rejecting Clearview AI's position that it should have been allowed to scrape personal information found online to train its AI without consent.

While the findings in both decisions are restricted in their reach to Alberta and B.C., it would not be surprising to see other provinces adopt a similar standing in future litigation. These developments underscore the need to exercise heightened caution when using personal information, even if collected online, for AI training purposes.

How can organizations favour compliance in training their AI models?

Businesses should reassess the legal basis for using customer, employee, or publicly accessible data to train AI models, ensuring that consent, purpose limitation, and transparency requirements are clearly met and documented.

Foreign organizations should carefully examine whether there might exist a real link between their business and Canadians, triggering the application of provincial privacy laws.

As regulatory scrutiny intensifies, AI training practices should be treated as a core privacy-risk issue, requiring the same level of caution as other high-risk data-processing activities.

For more information:

- Alberta judgment opens the door to the legitimization of data scraping and AI model training (June 2025)
- The extraterritorial reach of B.C.'s privacy laws: Court upholds privacy commissioner's order against foreign AI company (March 2025)
- Regulatory expectations are accelerating faster than most boards realize (May 2025)
- Beyond BC: Court of Appeal upholds broad reach of provincial privacy laws (March 2026)

AI and cybersecurity: New threats to thwart

As reported in the G7 Cyber Expert Group Statement on Artificial Intelligence and Cybersecurity, AI tools can strengthen defences by automating anomaly detection, fraud prevention, and incident response, but they also introduce significant new risks.

For example, AI can be leveraged to amplify the scale and sophistication of cyberattacks, craft hyper-personalized phishing campaigns, automate exploit development, and create adaptative malware.

In its Ransomware Threat Outlook 2025-2027, the Canadian Centre for Cyber Security warns that threat actors are adopting AI to lower technical barriers, making it easier for less skilled criminals to launch ransomware and extortion campaigns. From 2021 to

2026, the Centre observed a 26 per cent average year-over-year increase in reported incidents. This trend is only expected to accelerate in 2026.

In 2025, an increasing number of organizations deployed agentic AI systems, which should continue to expand this year. As opposed to other types of AI, agentic AI is defined by its ability to act autonomously and make decisions without direct human oversight.

Consequently, these AI agents increase the complexity and unpredictability of cyber threats, as they may inadvertently expose sensitive data, be manipulated through prompt injection or data poisoning, or become direct targets for attackers seeking to exploit vulnerabilities in AI design and training data.

How can organizations prepare for AI-related cyber threats?

Businesses should update their cyber risk frameworks and security controls to account for AI-specific threats, including AI-driven phishing, automated malware, and the exploitation of AI models through prompt injection or data poisoning.

Organizations deploying agentic or autonomous AI systems in particular should implement enhanced safeguards, including stricter access controls, continuous monitoring, and clear human-in-the-loop escalation mechanisms.

For more information:

- Readiness is your best cyber defence (May 2025)
- Privacy and cybersecurity are no longer IT issues, they are board issues (Sept. 2025)

BLG can assist

As one of the most respected Privacy & Cybersecurity teams in Canada, we have leading expertise on AI matters, and can provide you with tailored advice and actionable solutions to mitigate potential risks.

Let’s work together to make 2026 a year where innovation meets compliance.

By

Hélène Deschamps Marquis, Frédéric Wilson, Marianne Bellavance

Expertise

Cybersecurity, Privacy & Data Protection, Compliance with Privacy & Data Protection, Information Technology, Artificial Intelligence (AI)

BLG | Canada's Law Firm

As the largest, truly full-service Canadian law firm, Borden Ladner Gervais LLP (BLG) delivers practical legal advice for domestic and international clients across more practices and industries than any Canadian firm. With over 800 lawyers, intellectual property agents and other professionals, BLG serves the legal needs of businesses and institutions across Canada and beyond – from M&A and capital markets, to disputes, financing, and trademark & patent registration.

blg.com

BLG Offices

Calgary

Centennial Place, East Tower
520 3rd Avenue S.W.
Calgary, AB, Canada
T2P 0R3

T 403.232.9500
F 403.266.1395

Ottawa

World Exchange Plaza
100 Queen Street
Ottawa, ON, Canada
K1P 1J9

T 613.237.5160
F 613.230.8842

Vancouver

1200 Waterfront Centre
200 Burrard Street
Vancouver, BC, Canada
V7X 1T2

T 604.687.5744
F 604.687.1415

Montréal

1000 De La Gauchetière Street West
Suite 900
Montréal, QC, Canada
H3B 5H4

T 514.954.2555
F 514.879.9015

Toronto

Bay Adelaide Centre, East Tower
22 Adelaide Street West
Toronto, ON, Canada
M5H 4E3

T 416.367.6000
F 416.367.6749