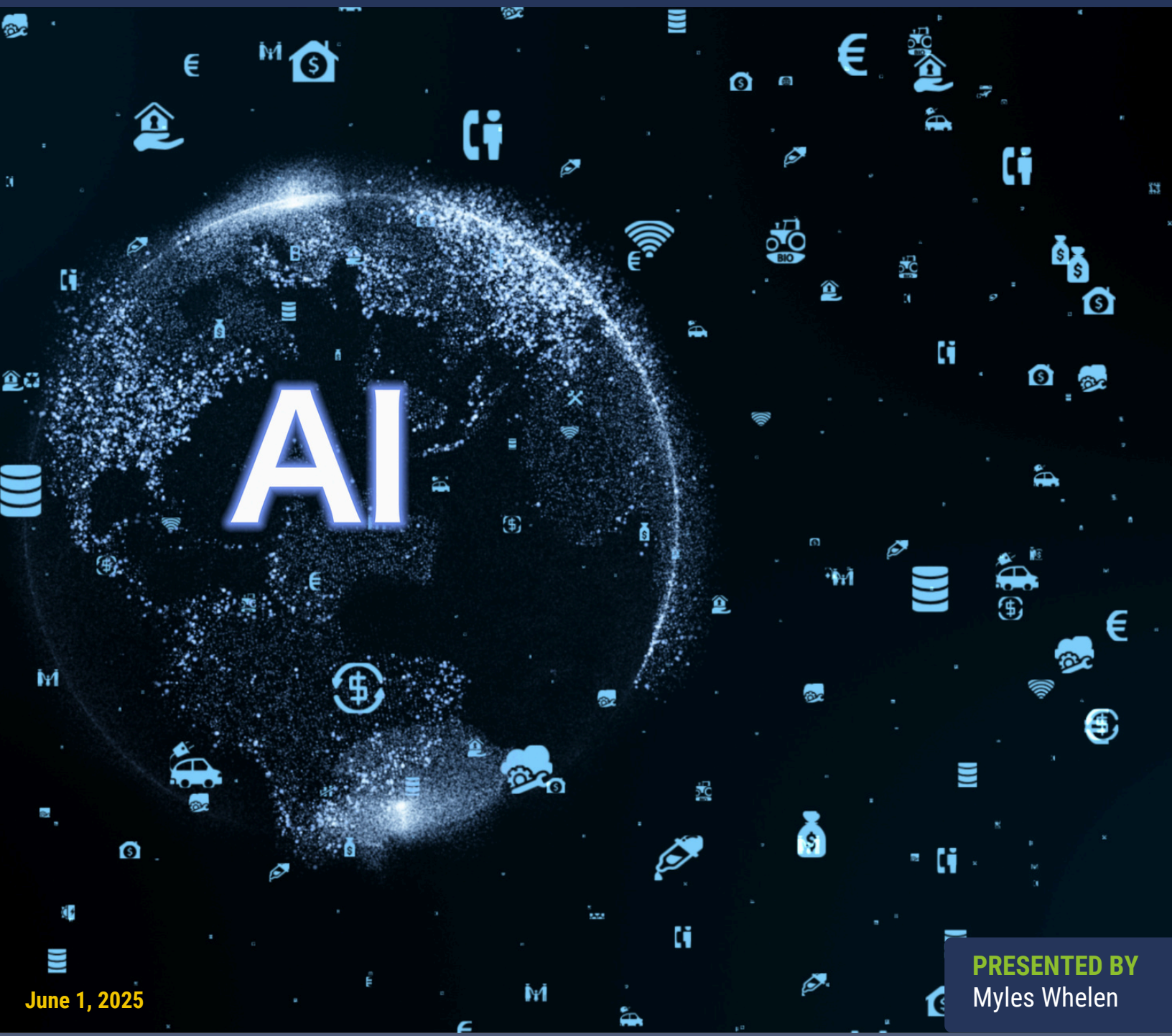
EU AI ACT:
IMPLICATIONS IN THE FINANCIAL SERVICES, LEGAL SERVICES, AND EDUCATIONAL SECTORS



June 1, 2025

PRESENTED BY
Myles Whelen

Future of Law Lab
University of Toronto Faculty of Law

FUTURE OF LAW

UNIVERSITY OF TORONTO FACULTY OF LAW

About the Future of Law Lab

The Future of Law Lab is a platform for students, academics, lawyers, and other professionals to participate in collaborative initiatives exploring how the law will evolve in the future. We will dive into the intersection of law, technology, innovation, and entrepreneurship, with programing dedicated to each of these streams. As a hub of interdisciplinary activity, we are dedicated to bringing together individuals from all backgrounds to examine the changing face of the legal profession.

This report outlines the key features of the EU AI Act—the first comprehensive regulation of artificial intelligence—and analyzes its implications for the financial services, legal, and educational sectors. It highlights the Act's risk-based framework, sector-specific obligations, and its impact on innovation, data protection, and AI governance, while drawing parallels with Canada's proposed Artificial Intelligence and Data Act.

About the University of Toronto Faculty of Law

Established in 1887, the Faculty of Law is one of the oldest professional faculties at the University of Toronto, with a long and illustrious history. Today, it is one of the world's great law schools, a dynamic academic and social community with more than 50 full-time faculty members and up to a dozen distinguished short-term visiting professors from the world's leading law schools, as well as 600 undergraduate and graduate students.

The Faculty's rich academic programs are complemented by its many legal clinics and public interest programs, and its close links to the Faculty's more than 6,000 alumni, who enjoy rewarding careers in every sector of Canadian society and remain involved in many aspects of life at the law school.

EU AI Act: Implications in the Financial Services, Legal Services, and Educational Sectors

The EU AI Act is the world's first comprehensive, non-sector-specific regulatory legislation for artificial intelligence.[1] The EU AI Act aims to improve the functioning of the EU Internal Market by promoting the development and uptake of "human-centric" and "trustworthy" AI tools.[2] The Act aims to balance innovation with the protection of health, safety, and the fundamental rights protected by the EU Charter.[3] Canada is currently aiming to implement similar legislation, the *Artificial Intelligence and Data Act.*[4] AIDA was heavily inspired by the EU AI Act and aims to be inter-operable with it.[5]

Overview

The Act applies to all AI systems, and imposes obligations on providers, deployers, importers, and distributors. AI systems are defined as "machine-based system[s] that [are] designed to operate with varying levels of autonomy and that may exhibit adaptiveness after deployment, and that, for explicit or implicit objectives, infer, from the input [they] receive, how to generate outputs such as predictions, content, recommendations, or decisions that can influence physical or virtual environments".[6] This definition is broad, but aims to be aligned with those used by other international organizations, and to clearly distinguish AI from standard computational systems.[7]

The Act follows a risk-based approach, classifying AI systems as "minimal risk", "transparency risk", "high risk", and "unacceptable risk". Additional requirements are imposed on AI systems designated as "general purpose" (GPAI). Systems carrying unacceptable risk are prohibited by the Act and are required to have been phased out within six months of the Act's

---

[1] EU, *Regulation 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (Artificial Intelligence Act)*, [2024] OJ, L 2024/1689 [EU AI Act].
[2] *Ibid,* art 1(1).
[3] *Ibid*.
[4] Bill C-27, *An Act to enact the Consumer Privacy Protection Act, the Personal Information and Data Protection Tribunal Act and the Artificial Intelligence and Data Act and to make consequential and related amendments to other Acts*, 1st Sess, 44th Parl, 2022 (second reading 24 April 2023).
[5] Innovation, Science and Economic Development Canada, *The Artificial Intelligence and Data Act (AIDA) – Companion document* (Ottawa: ISEDC, 2025) online: https://ised-isde.canada.ca/site/innovation-better-canada/en/artificial-intelligence-and-data-act-aida-companion-document.
[6] EU AI Act, *supra* note 1, art 2(1).
[7] *Ibid*, recital 12.

implementation (i.e., by February 2025).[8] Most of the Act lays out regulations for AI systems designated as "high risk".

Enforcement will begin gradually in the three years following the enactment of the Act, with all provisions in force by 2027.[9]

Unacceptable Risk

Prohibited applications of AI under the Act include systems that:[10]

- Use purposefully manipulative or deceptive techniques to materially influence human behaviour
- Exploit vulnerabilities due to age, disability, or socioeconomic status in order to influence human behaviour
- Use any form of "social scoring" leading to detrimental or unfavourable treatment that is disproportionate, unjustified, or outside the context in which the data was originally collected
- Assess/predict the risk of someone committing a criminal offence based solely on profiling or assessing their personality traits
- Create or expand facial recognition databases through untargeted scraping of images from the internet or CCTV footage
- Infer emotions in the workplace and educational institutions, except systems strictly used for medical or safety reasons
- Use biometric data to infer race, political opinions, union membership, religious or philosophical beliefs, sexual orientation; does not apply to filtering of lawfully acquired data or to categorization of data by law enforcement
- Enable law enforcement to use "real-time" remote biometric data, with some limited exceptions

[8] *Ibid*, art 5.
[9] *Ibid*, art 113.
[10] *Ibid*, arts 5(1)–5(2).

High Risk

AI systems considered "high risk" are subject to extensive regulation under the EU AI Act. There are two broad categories of systems considered high risk: (1) those that are safety components of products (or themselves products) covered by EU harmonization legislation, and (2) those listed in Annex III of the Act.[11]

Products and sectors covered by EU harmonization legislation include machinery, toys, watercraft, lifts, radio equipment, explosive equipment, pressure equipment, cableways, fuel-burning appliances, medical devices, civil aviation, motor vehicles, and trains/railway equipment.[12]

Systems listed in Annex III include, among others:[13]

- Systems used in the educational space that determine access or admission to institutions, that evaluate learning outcomes, that assess the level of education an individual will be able to access, and those used for exam proctoring
- Systems that determine access to essential public and private services, including those that evaluate eligibility for public benefits, those that evaluate creditworthiness or calculate credit score (systems used for detecting fraud excepted), those used for risk assessment and pricing of health and life insurance, and those used to evaluate/classify emergency responses (such as emergency calls or hospital triage)
- Systems used by judicial authorities or on their behalf to assist judicial authorities in researching and interpreting facts/law and applying law to facts, and systems used for influencing the outcome of elections or voting behavior

High-risk AI systems are required to meet numerous requirements, and various obligations are imposed on both producers and deployers of high-risk systems. All high-risk systems must be registered in an EU-wide database and are required to employ a risk management system.[14] Data is required to be gathered throughout the lifecycle of the system to assess its risks to health,

[11] *Ibid*, art 6(1).
[12] *Ibid*, annex I.
[13] *Ibid*, annex III, art 6(2).
[14] *Ibid*, arts 9, 71.

safety, and fundamental rights.[15] High-risk systems must also meet data governance standards, come with detailed technical documentation, and provide for effective human oversight.[16] All systems must "achieve an appropriate level of accuracy, robustness, and cybersecurity".[17] Accuracy metrics should be disclosed in the use instructions included with any AI system.[18] Systems must be resilient to errors, faults, or inconsistencies, and to third-party attempts to interfere with either outputs or training data.[19] Automatic recording of events must be built into all high-risk systems.[20] Providers of high-risk systems are required to take corrective action if they believe they are not in compliance with any regulation under the Act.[21] All high-risk systems must undergo a conformity assessment, including, in some cases, a fundamental rights impact assessment.[22]

Regulatory standards for high-risk AI systems will be developed over time via collaboration between regulators, industry participants, consumer organizations, and environmental and social stakeholders.[23] Once developed, a presumption of compliance will apply for any systems that meet the standards.[24]

Obligations imposed on deployers of high-risk systems include human oversight, monitoring, and data-keeping requirements.[25] Deployers may be required to undergo a data protection impact assessment.[26] Deployers that operate systems that make decisions or assist in making decisions in relation to natural persons are required to disclose that those persons may be subject to use of a high-risk AI system.[27]

---

[15] *Ibid*, art 9.
[16] *Ibid*, arts 11–12, 14.
[17] *Ibid*, art 15(1).
[18] *Ibid*, art 15(3).
[19] *Ibid*, art 15(4).
[20] *Ibid*, art 12.
[21] *Ibid*, art 20.
[22] *Ibid*, arts 27, 43.
[23] *Ibid*, arts 40-41.
[24] *Ibid*, art 42.
[25] *Ibid*, art 26.
[26] *Ibid*, art 26(9).
[27] *Ibid*, art 26(11).

Transparency Risk

Providers and deployers of chatbots must disclose to users that they are interacting with an AI system.[28] Providers and deployers must disclose that synthetic audio, image, video, or text content is AI-generated.[29] Any emotion recognition or biometric system must also be disclosed to users.[30] These requirements do not apply to legitimate uses in the law enforcement context.[31]

Minimal Risk

No additional requirements (beyond those imposed by existing laws) are imposed on systems carrying minimal risks. These include applications such as spam filters.[32]

General-Purpose AI Models (GPAI)

GPAI is defined as "an AI model trained with a large amount of data capable of self-supervision at scale, that displays significant generality and is capable of competently performing a wide range of distinct tasks regardless of the way the model is placed on the market and that can be integrated into a variety of downstream systems or applications".[33] GPAI models will be deemed to carry "systemic risk" in situations where it has "high impact capability" based on size of data set, number of users, and/or computing power.[34] Providers of any GPAI model are required to keep and make publicly available detailed technical documentation, respect EU copyright directives, and publish a detailed summary of content used for training. Providers of models that carry systemic risks are required to test their models in accordance with standardized protocols, continually assess and mitigate risks, document and report serious incidents, and ensure adequate levels of cybersecurity protection.[35] Harmonization standards will gradually be developed for GPAI models.

---

[28] *Ibid*, art 50(1).
[29] *Ibid*, art 50(2).
[30] *Ibid*, art 50(3)
[31] *Ibid*, art 50(1).
[32] Tambiama Madiega, "Artificial Intelligence Act", *European Parliamentary Research Service*, Members' Research Service PE 698.792 (September 2024) at 9.
[33] EU AI Act, *supra* note 1, art 3(63).
[34] *Ibid*, art 51.
[35] *Ibid*, art 53.

Innovation

The Act aims to balance protection of health, safety, and fundamental rights with innovation and encouragement of adoption of AI.[36] To facilitate this goal and promote harmonization in the AI space, the Act mandates the creation of at least one regulatory sandbox in each member state of the EU in which experimental AI systems can be explored and tested for a limited time under the close supervision of regulators; these sandboxes are to be operational by August 2026.[37]

The sandboxes aim to improve legal certainty in achieving regulatory compliance with the Act, facilitate best practices, fostering innovation and competitiveness, and facilitate access to the EU market for AI systems, particularly for start-ups.[38] Competent authorities will provide regular reports to the EU AI office throughout the process.[39] Rules around personal data use are somewhat relaxed within the sandbox scheme, provided certain conditions are met.[40] A process also exists for testing high-risk AI systems in the real world outside of the sandbox scheme by application to the Commission.[41]

Implications in the Financial Services Sector

AI is already employed in numerous ways in the financial services sector. These include virtual advisor/chatbot services, AI-assisted credit and risk scoring, algorithmic trading, asset allocation, asset price forecasting, capital optimization, and market impact analysis.[42]

High-risk AI systems listed in Annex III of the EU AI Act that directly affect the financial services industry include systems that evaluate creditworthiness or calculate credit score and those used for risk assessment and pricing of health and life insurance. Any system used exclusively for fraud detection or for anti-money laundering purposes is explicitly excluded from high-risk status under the Act.[43]

---

[36] *Ibid*, art 1(1).
[37] *Ibid*, art 57.
[38] *Ibid*, recital 137.
[39] *Ibid*, art 57.
[40] *Ibid*, art 59.
[41] *Ibid*, art 60.
[42] See Patrick Mingnault & Stéphane Rousseau, "Guardrails for the Deployment of AI in Finance in Canada: Where Do We Go from Here?" (2024) 41:1 BFLR 1.
[43] EU AI Act, *supra* note 1, recital 58.

Loan decisions and credit scoring are therefore heavily implicated by the AI Act. Given that a creditworthiness assessment will almost always involve personal profiling to some degree, these applications of AI will usually fall into the high-risk category. EU-based financial institutions already report using AI for customer profiling and are therefore directly touched by the Act.[44]

The obligations around high-risk AI systems apply to financial institutions whether they are deployers or providers. The Act mandates that all providers and deployers of AI systems must ensure a sufficient level of AI literacy in their staff.[45] The risk management, conformity assessment, and technical documentation provisions of the Act apply to financial institutions and financial technology (fintech) companies. Providers or deployers that are financial institutions are granted certain explicit derogations under the Act; many of the requirements around record-keeping, risk management, and monitoring can be satisfied via compliance with existing EU financial regulatory law.[46] Commentators have noted that autonomous systems have been used for decades in the financial services industry for several purposes, including credit scoring; the Act does not necessarily grandfather in exceptions for these systems and they will still be required to undergo a conformity assessment.[47]

As in any other industry, any form of generative AI that consumers interact with (e.g., chatbots, robo-advisors) is subject to disclosure requirements.[48]

Regulatory sandboxes are familiar to the fintech industry. The first fintech sandbox launched in the UK in 2016 and numerous jurisdictions (including the EU) have employed them since then.[49] The AI regulatory sandbox presents novel challenges, as there is no one "AI industry".[50] However, the AI regulatory sandboxes will present opportunities for the fintech industry to explore novel AI technologies and play an active role in developing regulations for use of AI by financial institutions.

---

[44] https://www.eba.europa.eu/publications-and-media/publications/special-topic-artificial-intelligence
[45] EU AI Act, *supra* note 1, art 4.
[46] *Ibid*, art 26.
[47] Aviv Gaon & Yuval Reinfeld, "The Implications of the EU's New AI Regulation: A Comprehensive Analysis for Canada" (2024) 36 IPJ 235 at 247.
[48] EU AI Act, *supra* note 1, art 50.
[49] Ryan Nabil, "Artificial Intelligence Regulatory Sandboxes" (2024) 19:2 JL Econ & Pol'y 295 at 296.
[50] *Ibid* at 303.

Finally, the AI Act interacts with existing EU financial and data protection regulations, including the General Data Protection Regulation ("GDPR").[51] The GDPR requires that data collected be adequate, relevant, and limited to what is necessary for the purpose.[52] Given the highly sensitive nature of financial data, this is a particular concern in this sector.

Implications in the Legal Services Sector

The Act defines "systems used by judicial authorities or on their behalf to assist judicial authorities in researching and interpreting facts/law and applying law to facts" as high-risk.[53] Private lawyers and law firms are likely not considered "judicial authorities", but any AI system designed for use by judges and other court officials is covered by this heading. Additionally, the Act clarifies that such systems are also considered high risk when used by alternative dispute resolution professionals in cases where they have the capacity to make legally binding decisions.[54] Developers of such systems must meet all obligations for providers of high-risk systems, and Courts and ADR providers that use these systems would be subject to all obligations for deployers.

AI systems already used by law firms and lawyers include assisted research tools, assisted drafting tools, predictive analysis tools to analyze past case data, as well as chatbot-type tools to answer basic client questions.[55]

Obligations around ensuring sufficient AI literacy in staff apply to law firms as well. The Law Society of Ireland has released guidelines for firms using AI tools, including assessing existing knowledge, designing tailored training, maintaining comprehensive training records, and regularly updating training to reflect new developments in AI technologies.[56]

---

[51] EU, *Regulation 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC*, [2016] OJ L 119 [GDPR].
[52] *Ibid*, art 5(1)(c).
[53] EU AI Act, *supra* note 1, annex III(8)(a).
[54] *Ibid*, recital 61.
[55] Jennifer J Cook & Denista R Mavrova Heinrich, "AI-Ready Attorneys: Ethical Obligations and Privacy Considerations in the Age of Artificial Intelligence" (2024) 72:3 U Kan L Rev 313 at 321–28; see also Sarah A Sutherland, "AI use skyrocketing at North American law firms", *CBA National Magazine* (4 November 2024), online: https://nationalmagazine.ca/en-ca/articles/legal-market/legal-tech/2024/ai-use-skyrocketing-at-north-american-law-firms.
[56] Law Society of Ireland, "Navigating the EU AI Act: ensuring AI literacy in legal practices" (10 December 2024), online: https://www.lawsociety.ie/news/news/Stories/navigating-the-eu-ai-act-ensuring-ai-literacy-in-legal-practices.

Client data is highly personal and confidential. There are therefore interactions between the GDPR and the AI Act in the legal services sector as well; any systems trained on or with access to client data are subject to data protection regulations.

There is considerable uncertainty around liability under the EU AI Act. This is relevant across all sectors, but perhaps particularly so in the legal services sector where documented cases of misuse have already occurred. Although assisted research and drafting technologies are advancing, incidents have already occurred around the world of generative AI "hallucinating" cases or statutes, leading to liability for lawyers and firms, as well as professional misconduct allegations.[57] The EU had intended to implement additional legislation on AI liability to complement the AI Act, but in February 2025, the bill was withdrawn, citing a lack of consensus on core issues.[58] There is currently no clear path forward on AI liability.

As in the financial sector, the regulatory sandbox scheme and other measures supporting innovation within the Act will present opportunities for legal tech providers and law firms deploying AI tools to explore new technologies and play an active role in the development of regulations.

Educational Space

AI presents novel opportunities in the classroom and is rapidly challenging traditional paradigms in the educational sector. Commentators have noted that AI tools have the potential to address learning challenges and make education more accessible and inclusive.[59] AI is adaptable to learning needs and can be tailored to specific needs, strengths, and weaknesses.[60] However, concerns around the overuse of data, profiling of learners, and harms of algorithm-driven discrimination remain.[61] Though tools will improve over time, generative AI often still makes mistakes. As noted by one commentator, AI is only as good and reliable as the data it is

---

[57] See *Zhang v Chen*, 2024 BCSC 285; *Ko v Li*, 2025 ONSC 2766; *Harber v The Commissioners for HMRC*, [2023] UKFTT 1007 (TC).
[58] EU, *ANNEXES to the COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT, THE COUNCIL, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS*, COM (2025) 45 final at 26 online: https://commission.europa.eu/document/download/7617998c-86e6-4a74-b33c-249e8a7938cd_en?filename=COM_2025_45_1_annexes_EN.pdf.
[59] Sandra Fabijanic Gagro, "Artificial Intelligence in Education - Current Challenges" [2024] 2024 Annals Fac L Belgrade Int'l Ed 725 at 729.
[60] *Ibid* at 730.
[61] *Ibid* at 731–32.

trained on and is only as ethical as its creator.[62] Concerns remain around biases and inequalities present in the education system being exacerbated by AI.[63] Manipulation of data, "deepfake" images and videos, and "hallucinations" of false information are particular concerns in the educational sector given the vulnerabilities of children.[64]

"High-risk" AI applications in the educational space include systems that determine access or admission to institutions, that evaluate learning outcomes, that assess the level of education an individual will be able to access, and those used for exam proctoring. Obligations apply to educational tech companies as providers and educational institutions as deployers of AI technologies.[65] Additionally, AI-based emotional and biometric analyses in educational institutions are explicitly prohibited under the Act.[66]

Applications of AI in the educational space that would likely fall into the "transparency risk" category include AI tutors and other content generators.[67] Again, users would need to be told that they are interacting with AI. Systems that collect personal data would be required to comply with GDPR.

As in other sectors, mandatory AI literacy training will become relevant in the educational space for schools and other organizations using AI tools. Some countries have begun to issue guidance on this. For instance, Kennisnet in the Netherlands (a government-funded organization dedicated to ICT in education) has begun to issue guidelines for AI use in schools and to ensure that both educators and students meet the literacy requirements under the AI Act.[68]

---

[62] *Ibid* at 734, citing Andre M Perry and Nicol Turner Lee, "AI is coming to schools, and if we're not careful, so will its biases" (26 September 2019), online: https://www.brookings.edu/articles/ai-is-coming-to-schools-and-if-were-not-careful-so-will-its-biases/.
[63] Fabijanic Gagro, *supra* note 58 at 734, citing Tufan Adiguzel et al, "Revolutionizing education with AI: Exploring the transformative potential of ChatGPT" (2023) 15:3 Contemporary Educational Tech ep429.
[64] Fabijanic Gagro, *supra* note 58 at 734, citing Wayne Holmes et al, *Artificial Intelligence and Education: A Critical view through the lens of human rights, democracy and the rule of law* (Strasbourg: Council of Europe, 2022).
[65] EU AI Act, *supra* note 1, annex III(3).
[66] *Ibid*, art 5(1)(f)
[67] Fabijanic Gagro, *supra* note 58 at 730, 740.
[68] Loes van Zuijdam, "Voldoen aan de AI-verordening" (last modified 7 May 2025), online: https://www.kennisnet.nl/artificial-intelligence/voldoen-aan-de-ai-verordening/.

Finally, the regulatory sandboxes and other provisions fostering innovation will present novel opportunities in the EdTech sector and allow the industry to actively shape the development of regulations.

Future of Law Lab

University of Toronto Faculty of Law