AI Acts in Focus: Comparative Insights from the European Union and Canada for India's Policy Evolution

[1]Shivam Bharal* and [2]Ritu Sharma

[1,2]Sardar Patel University of Police, Security and Criminal Justice, Jodhpur, India
23lm18@policeuniversity.ac.in

Abstract. This paper assesses and compares the European Union's 'Artificial Intelligence Act, 2024' with Canada's 'Artificial Intelligence and Data Act, 2022.' It investigates imperative components of both the AI Acts, like risk-oriented frameworks, ethical standards, innovation incentives, and compliance systems. Considering that India has emerged as a major force in artificial intelligence research and development, the study highlights the necessity of utilizing the legislative frameworks of other countries to develop a regulatory strategy that harmonizes with the socio-economic and technological needs of its citizens. The research covers a range of recommendations, including establishing AI sandboxes & risk-management systems, running community awareness campaigns, and enforcing resilient data protection legislation. Furthermore, it accentuates the significance of cooperation between governmental departments, academia, and business stakeholders to intensify innovation while maintaining responsibility. Such magnified understanding is anticipated to help India find a 'catalyzing' middle ground between the requirement for AI innovation and ethical and societal safeguards.

Keywords: Artificial Intelligence, Regulation, EU AI Act, AIDA, Policy Framework, Compliance.

1 Introduction

Artificial Intelligence (AI) has become a pervasive technology, propelling significant advancements across various fields, including healthcare, education, governance and finance [1]. However, the rapid and widespread adoption of AI also brings numerous disputes, including privacy violations, inherent biases, ethical concerns, and unregulated implementation. This emphasizes the significance of having a legislative framework that not only standardizes and regulates AI but also creates a setting where innovative practices can prosper without redundant limitations. Across the globe, 'Artificial Intelligence Act (AI Act), 2024'[2] of the European Union and 'Artificial Intelligence and Data Act (AIDA), 2022'[3] of Canada are the most exceptional and contemporary AI regulatory laws.

N. Vyas et al. (eds.), *Proceedings of the International Conference on Advancements in Computing Technologies and Artificial Intelligence (COMPUTATIA 2025)*, Advances in Intelligent Systems Research 189,
https://doi.org/10.2991/978-94-6463-700-7_20

India, as a dynamic hub for some of the most rapidly advancing technology ecosystems globally, holds a promising position to lead and shape the future of innovation in AI [4]. Its flourishing technology sector, skilled workforce and growing commitment to advanced research, helps to drive transformative progress in AI on the world stage. However, no formal regulatory structure governs AI in India, and critical ethical, legal and social questions remain unaddressed. This paper reviews the approaches taken by the EU and Canada, identifies available lessons and makes policy recommendations for India, based on its domestic socio-economic context and developmental priorities.

2 Examination of key frameworks

2.1 Artificial Intelligence Act, 2024 (European Union)

Context and Objectives. The European Union's Artificial Intelligence Act (AI Act) is the first landmark legislation to ensure a consistent and harmonized regulatory environment where artificial intelligence deployed across all EU member states will be regulated [5]. On March 13, 2024, the European Parliament passed it and on August 1, 2024, it was implemented. Motivated by the need to ensure ethical and responsible development and use of AI, the Act focuses on minimizing potential dangers while also encouraging innovation and promoting a competitive AI market in Europe[6]. Central to the AI Act is a risk-based approach; not all AI systems pose the same threat.

Ethical Framework, Measures in support of Innovation (Chapter VI), and Enforcement (Chapter VII). The AI Act is strongly grounded in the ethical principles set forth in the 'Charter of Fundamental Rights of the European Union'[7]. What this means is that the legislation is focused on fairness, accountability, transparency, and non-discrimination in AI systems. The EU understands that to encourage innovation and scale up its AI sector, it must act and to this end, the Act contains provisions for "regulatory sandboxes."[8] These are regulated environments that allow SME's and other AI developers to explore cutting edge AI applications, in a supervised setting which allows for the development and enhancement of their systems without the regulatory risk associated with the early developmental stages.

This regulatory framework is supervised by the 'European Artificial Intelligence Board' established under Article 65 of the Act**,** a decentralized committee that coordinates the activities of 'National Competent Authorities' established under Article 70 of the Act, throughout the member states. The importance that the EU ascribes to effective enforcement and compliance is further evidenced by the strong financial penalties prescribed under Article 99 of the Act, for non-compliance with the AI Act, which can reach up to €35 million or up to 7% of a company's global annual revenue. The law also includes provisions for a right to redress of people harmed by non-conforming AI systems [9].

Risk-Based Classification. The AI Act establishes a 'Risk-Based Classification Mechanism'[10] which places AI systems into one of four tiers – Prohibited Practices (Chapter II, AI Act), High Risk AI Systems (Chapter III, AI Act), Limited Risk AI Systems (Chapter IV, AI Act) and Minimal Risk AI Systems (Chapter V, AI Act). The Fig. 1 explains these four tiers of AI systems according to their estimated level of risk.

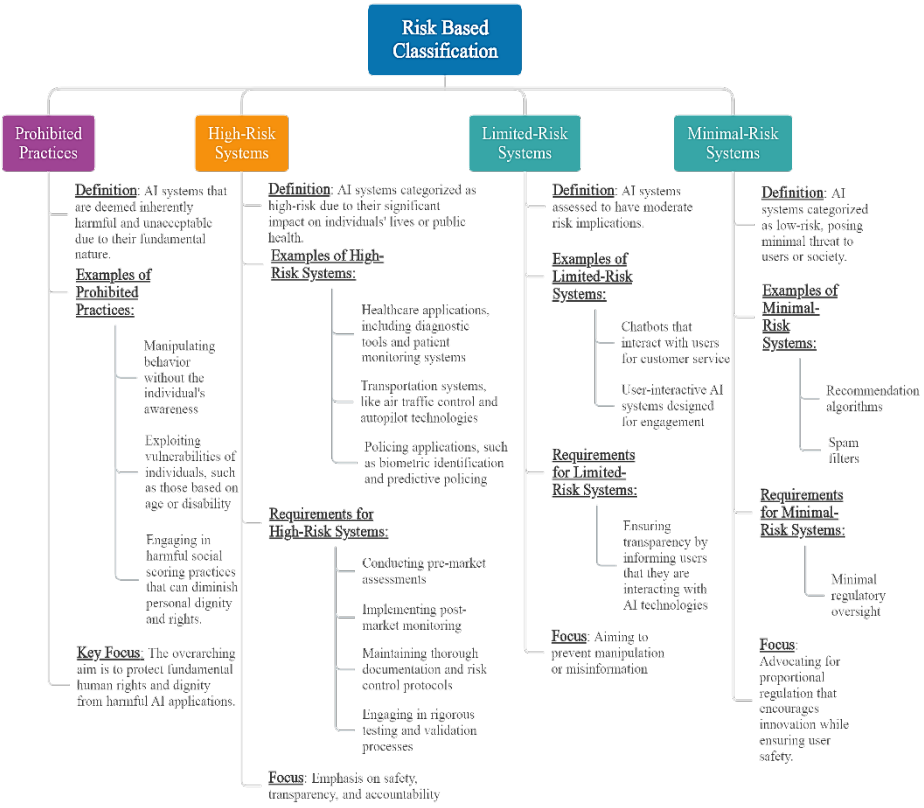

Fig. 1. Risk-based classification of AI systems under EU AI Act

Limitations and Criticism of the Act. While the act sets important standards for safety and ethical considerations, there are still certain limits and deficiencies in it that make critics attack with vigorous shots at whatever seems most vulnerable. Some of them are given below.

- Scope of Application and Ambiguity in Definitions: The Act does not monitor the pre-launching, research or development stages of AI systems, before entering the market. This expulsion may allow AI technologies which could prove to be dangerous if developed outside of proper monitoring in critical early stages of development. Also, the definitions in a legislation must be unambiguous. Some terms, such as

"high-risk AI systems," lack certainty, which results in making different interpretations and consequently, the enforcement differs. This indefiniteness can be a complication to compliance.

- Potential for Overregulation and Inflexibility: Most of the startups and smaller organizations could find the strict conditions and restrictions very difficult to meet the requirements for conformity, which might hamper the progress in new technologies. Critics states that these conditions and overregulation in the AI regulations may stifle innovation. The regulatory system may also become outdated and create intolerable burdens on well-established as well as growing organizations in this business field, during the evolution of new technologies. Regulation's inflexible structure may not suit AI's fast developing pace.
- Limited stakeholders' engagement and conformity assessment delays: The regulation may not sufficiently reflect the interests of all stakeholders, including businesses, civil society, and directly impacted communities, due to their inadequate engagement in the development and implementation process of AI systems. As a consequence, policy could just be developed without considering the distinctions of AI technologies. It also allows for a limited period of authorization while conformity assessment procedures are being carried out[11]. Critics argue that this could lead to delays in ensuring that AI systems make necessary safety and ethical standards, potentially putting individuals at risk during this interim period.

2.2 Artificial Intelligence and Data Act, 2022 (Canada)

Context and Goals. Bill C-27, or the 'Digital Charter Implementation Act, 2022' is currently under committee review stage in Parliament of Canada (House of Commons)[12]. It consists of various privacy-related statutes, including the 'Artificial Intelligence and Data Act (AIDA)'. According to Sec 4(a) of AIDA, the Act is mainly constructed to control AI usage more broadly across interprovincial and international trade and commerce. Its purpose is to institute a responsible and balanced AI governance framework, which assures that AI systems are deployed in a transparent and accountable manner within Canada's marketplace, acknowledging ethical requirements as well. Section 4 (b) of AIDA places emphasis on risk-management exclusively to eradicate harm from high-impact AI applications that would considerably affect individuals.

Emphasis on High-Impact Systems. According to Section 5(1) of AIDA, the Act regulates what it considers "high-impact systems", which are AI systems that could significantly affect the safety, rights, or economic well-being of natural persons in a society. Many of these applications fall under the same legal conceptual framework, and legislative attentiveness is needed for the use of AI in hiring, credit scoring, and essential services. Complicated risks may bring some AI systems which need careful deliberation, while minimal threats may require quick intervention. AIDA promotes balancing innovation and protection through clear communication about systems' intent, function, and relevant safeguards[13].

Compliance Requirements. For high-impact systems, AIDA forms material compliance requirements. This includes the following requirements.

- Assessment Necessity and Risk Direction: Section 7 of AIDA provides for assessment necessity. People or corporation in charge of AI systems have the responsibility to determine if their system qualifies as a high-impact AI system. This evaluation must be conducted in accordance with the regulation. Section 8 of AIDA provides for risk direction. System owners and operators must identify, assess, and reduce potential hazards of harm or biased outputs that may arise from the use of high-impact AI systems. Mitigation actions must be observed to determine their productivity.
- Record-Keeping and Notification of Damage: Section 10 of AIDA emphasizes that detailed records must be kept by organizations engaged in regulated activities related to high-impact systems. The rules necessitate general descriptions of activities and supplementary records. Section 12 of AIDA explains that if a high-impact AI system causes, or is likely to cause material harm, the responsible person must notify the Minister immediately. Therefore, it substantiates that any kind of potential issue can be addressed effectively.
- Monitoring of mitigation measures and regulatory supervision: Section 9 of AIDA underscores that a person who is responsible for a high-impact system must, in accordance with the regulations, establish measures to monitor compliance with the mitigation measures they are required to establish under Section 8 and the effectiveness of those mitigation measures. Section 15 of AIDA provides that audits and procedures to cope with recognized risks or contraventions related to high-impact systems can be necessitated by the Minister. Ensuring adherence and safety is essential for this oversight.

Enforcement. The AIDA establishes strict sanctions for non-compliance. Organizations that violate the laws could be fined up to 10 million Canadian dollars or up to 3% of their total annual global revenues, which demonstrates Canada's commitment to ensure accountability and responsible advancement, with an enforcement that encourage companies to focus on ethical creation and use of transformative AI[14]. As Section 38 of AIDA, which addresses unlawful possession or usage of personal information and Section 39 of AIDA, which provides for making of a system available for unauthorized use, punishment is also determined for general offences relating to Artificial Intelligence systems.

Section 40 outlines repercussions for violations of Section 38 and 39. For entities besides individuals, maximum indictable penalties involve a fine equaling the greater of 25 million Canadian dollars or up to 5% of total income from worldwide operations in the previous year, whereas summary convictions authorize maximum fines reaching the greater of 20 million Canadian dollars or up to 4% of such earnings. For people, indictable penalties potentially encompass fines at judicial discretion, imprisonment up to five years less one day, or both; on summary conviction, maximum fines attainable extend to 100,000 Canadian dollars, imprisonment up to two years less one day, or both may apply.

Limitations and Criticisms of the Act. The Canadian law regulating Artificial Intelligence systems has several limitations to regulate AI systems and guard individuals from potential afflictions, the weaknesses of definitions, scope, transparency mechanisms for complaints, relief programs give one pause. These last several issues may largely render the Act ineffective at achieving its purposes in protecting right of people before rapidly moving artificial intelligence.

- Scope of Application and Ambiguity in Definitions: Since the Act broadly defines an "Artificial Intelligence System," anyone can be confused about which specific technology or applications are included within its scope. The lack of clarity and unambiguity in definitions makes enforcement and compliance difficult. The Act does not apply to any government institution as defined in section 3 of the 'Privacy Act.' This exception implies that government bodies will not be held accountable for their use of AI programs and may operate without restraint or regulation, injuring citizens or whole segments of society at their pleasure.
- Limited Transparency Requirements and Focus on High-Impact Systems: Although the Act more or less requires publication of certain information, release of trade secrets is excluded. This might cut transparency and public credibility, as stakeholders would then have no way to find out important things about how systems made by AI operate and what effect they have. The Act fluctuates toward high-impact systems, but does not prescribe any clear criteria for doing so. This could mean that some truly significant AI systems slip through the cracks or are inadequately regulated, thereby endangering individuals and society at large.
- Potential for Overreach and delegation of powers: The widespread powers which the Minister and Governor in Council can exercise through regulations for enforcement of the Act might lead to overreach or else wrong use of authority. This could inhibit innovation, or impose unjust burdens on businesses which develop AI technologies. The Act also allows for the delegation of powers to enforce compliance, which may lead to inconsistencies in how regulations are applied. If delegated authorities lack the necessary expertise or resources, this could result in ineffective oversight of AI systems.

3 Comparative analysis

The comparison of the Artificial Intelligence and Data Act (AIDA), 2022 of Canada with the European Union's Artificial Intelligence Act (AI Act), 2024 aims to regulate, according to legal norms, the development, dissemination, and usage of artificial intelligence systems and to minimize risk while at the same time promoting creativity and observing ethical standards. Table 1 focuses on key features such as operational scope, jurisdiction, penalties, supervision, and protection of information. It lays out the two pieces of legislation's general orientations to trustworthy AI in sharp contrast—one with a broad view and one more concentrated.

Table 1. Comparative analysis of AI Act and AIDA

Aspect	EU AI Act	AIDA
Scope	Provides harmonized rules for AI systems to ensure safety, fundamental rights, and innovation in the EU.	Regulates interprovincial and international trade in AI systems and prohibits harmful AI-related practices.
Jurisdiction	Applies to providers and deployers within the EU and systems impacting individuals in the EU, including some external operators.	Applies to private-sector activities in Canada, excluding government institutions, national defense, and intelligence agencies.
Definition of AI	Systems capable of inferring patterns or making predictions based on machine-based learning or reasoning.	Systems using machine learning, neural networks, or similar techniques for decision-making or predictions.
High-Risk AI Systems	Imposes specific requirements for high-risk systems, including conformity assessments and post-market monitoring.	Requires assessment, risk mitigation, and transparency for high-impact systems.
Penalties and Fines	Violations can incur fines up to EUR 35 million or up to 7% of global revenue (whichever is higher).	Violations can result in fines up to CAD 10 million or up to 3% of global revenue (whichever is higher).
Punishment	No provision for Imprisonment; only penalties provided.	Provisions provided for Imprisonment in Section 40 (Punishment).
Exemptions	AI systems for military and national security purposes. Also excludes scientific R&D before market placement.	AI systems for national defense, security intelligence, and certain government activities.
Transparency	Mandates transparency for specific AI practices, including disclosure of AI system usage to affected individuals.	Requires publication of plain-language descriptions for high-impact systems.
Prohibited Practices	Bans practices such as social scoring, manipulative AI, and certain uses of biometric identification.	Prohibits certain AI practices causing serious harm or biased outcomes.
Governance	Establishes the European Artificial Intelligence Board for coordination and enforcement.	Minister of Industry oversees compliance, with powers to audit and impose penalties.
Data Protection	Aligns with GDPR and other EU data protection laws, emphasizing the safeguarding of personal data.	Includes measures for anonymization and confidentiality of data used in AI systems.
Innovation Support	Supports innovation through regulatory sandboxes and measures for SMEs.	Encourages responsible AI development within trade contexts.

4 Recommendations for policy-making on AI in India

Drawing insights from the Artificial Intelligence and Data Act (AIDA) of Canada and the Artificial Intelligence Act (AI Act) of EU, here are some recommendations for shaping AI policy in India most effectively.

4.1 Regulatory Sandboxes and Risk Management Framework

India can develop AI regulatory sandboxes in which new AI technology can be tested in a controlled terrain. This ensures that such technologies cleave to ethical norms and do not undermine public safety and security, which is something that cannot be done outside operating conditions of any kind. These regulatory sandboxes support market readiness and ensures that AI technologies must align with ethical, legal and societal expectations. Regulations which are suitable in accordance with the technological maturity and extent of threat, can be enforced on a case-by-case basis to handle the risks related to it. This moderating approach equilibriums innovativeness and detriment forestallment in equal measure.

4.2 Privacy, Transparency, Responsibility and Data Protection

Strict data protection laws can be established in India, to govern personal and private information of individuals, used in AI systems. All associations which violate these rules should be brought to the law, so as to make sure that they follow both norms of morality and law. In addition to that, AI systems, which can maintain a detailed 'log' in future should be made compulsory. AI policy must encourage transparency by requiring organizations to disclose when AI is being used, especially in public-facing applications[15]. Record-keeping of data will make it easier to track down their authors in cases of non-compliance or breakdowns. This will ensure accountability, transparency and helps in establishing a sense of responsibility.

4.3 Collaboration, Standardization and Public Awareness

India can promote cooperation among government, industrialists and academic institutions to establish the foremost AI development practices. These collaborative assemblages are designed to balance inventiveness with ethical considerations and security. It can also help in maintaining the benchmark of AI systems. Public awareness campaigns and training programs can be carried out in India, to increase AI knowledge and understanding among the general population. It can also enable stakeholders like government officers, non-profit organizations and private agencies, to understand AI's impact on society. It will also help in sensitization of India's diverse cultural and linguistic landscape.

4.4 Ethical AI integration across key sectors

India's AI policy must prioritize fairness, non-discrimination and respect for human rights throughout all sectors, to establish an ethical and human-centric AI [16]. AI tools, which specifically focused on education, should customize learning without negotiating the privacy of student's data, and in legal landscape, strict regulations are required to prevent misuse of surveillance and facial recognition technologies. AI systems must be carefully tested for accuracy and safety in healthcare sector. Comprehensive and sustainable AI, which is aligned with shared values can be promoted by India by embedding ethical principles into sector-specific guidelines. Fig. 2 represents major takeaways for making AI act in India.

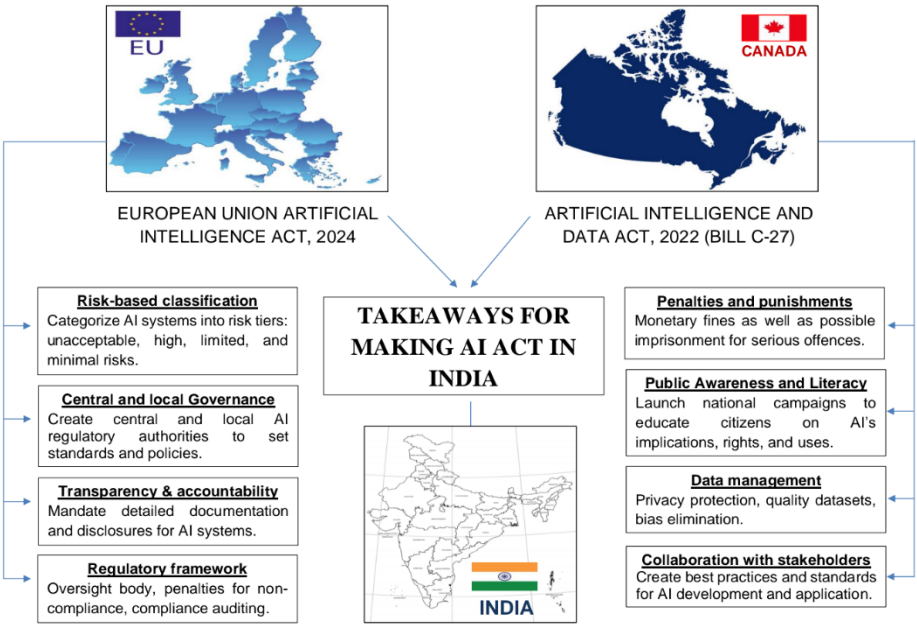

Fig. 2. Takeaways for making AI Act in India

4.5 Penalties and punishments for non-compliance

Serious breaches of AI regulations must be checked with strict penalties and punishments, which include both heavy fines and criminal liability. Corporate and individual accountability must be established through criminal liability for deceptive AI practices. A layered system of warnings, fines, and if not complied with it, then heavy punishments, will promote compliance with the AI regulation. A specialized AI tribunal should be established to adjudicate disputes. This will nurture public confidence in the legal system and encourage responsible AI innovation.

5 Conclusion

India, as a nation, is positioned to become the epicenter of AI innovation around the word[17]. However, there is currently no legislative framework in India, which regulates the use of AI[18]. The rapid advancement of AI presents both opportunities and challenges before it[19]. The expansion of AI technology simultaneously involves recognizing ethical, legal, and social concerns[20]. India can form an updated policy for controlling AI that cherishes innovation and defends the public interest as well, by extracting major features of the AI regulatory legislations of the European Union and Canada.

The European Union's AI Act emphasizes on a risk-based classification, which sets out certainly different types of AI systems[21]. Similarly, Canada's AIDA focuses on high-impact AI systems, which lay emphasis on measures of compliance such as risk assessments, warnings about possible threats and maintaining accounts. Both the Acts highlight the necessity for flawlessness, responsibility and severe penalties against any kind of non-conformity. Reliance, intelligence and acceptance of AI systems must be promoted through awareness drives and empowering representatives & stakeholders. Besides these recommendations, data protection have to be a foundation of India's AI policy.

Organizations must take the responsibility for the illegitimate use of any data and AI systems necessarily regard an individual's privacy. Eventually, India will have to set down extremely heavy penalties for non-compliance. To discourage frequent infringements and emphasize the graveness of righteous evolvement, these penalties should include voluminous fines, and in serious cases, detaining conspicuous perpetrators. Such a balanced approach will harmonize moral and social contemplations with innovation, through which, it is wholly within India's capability to make itself a global leader in AI development.

References

[1] A. Habbal, M. K. Ali, and M. A. Abuzaraida, "Artificial Intelligence Trust, Risk and Security Management (AI TRiSM): Frameworks, applications, challenges and future research directions," *Expert Systems with Applications*, vol. 240, p. 122442, Apr. 2024, doi: 10.1016/j.eswa.2023.122442.

[2] *Artificial Intelligence Act*, no. 1689. 2024. [Online]. Available: https://eur-lex.europa.eu/eli/reg/2024/1689/oj

[3] Minister of Innovation, Science and Industry, *C-27, Part 3 Artificial Intelligence and Data Act*, no. C–27. 2022. [Online]. Available: https://www.parl.ca/DocumentViewer/en/44-1/bill/C-27/first-reading

[4] S. Rana, P. Tyagi, R. N. A., G. Saleem, and V. Grover, "Innovations and Entrepreneurial Ecosystems for Sustainable Commercial Success: A Text Mining Approach," in *Advances in Logistics, Operations, and Management Science*, S. Trivedi, V. Grover, B. Balusamy, and A. Ganguly, Eds., IGI Global, 2024, pp. 183–211. doi: 10.4018/979-8-3693-5503-9.ch010.

[5] A. Gaon and Y. Reinfeld, "The Implications of the EU's New AI Regulation: A Comprehensive Analysis for Canada," *SSRN Journal*, 2024, doi: 10.2139/ssrn.4986407.

[6] C. Cancela-Outeda, "The EU's AI act: A framework for collaborative governance," *Internet of Things*, vol. 27, p. 101291, Oct. 2024, doi: 10.1016/j.iot.2024.101291.

[7] "Charter of Fundamental Rights of the European Union." Official Journal of the European Communities, Dec. 07, 2000. [Online]. Available: https://www.europarl.europa.eu/charter/pdf/text_en.pdf

[8] T. Buocz, S. Pfotenhauer, and I. Eisenberger, "Regulatory sandboxes in the AI Act: reconciling innovation and safety?," *Law, Innovation and Technology*, vol. 15, no. 2, pp. 357–389, Jul. 2023, doi: 10.1080/17579961.2023.2245678.

[9] "AI Act | Shaping Europe's digital future." Accessed: Feb. 06, 2025. [Online]. Available: https://digital-strategy.ec.europa.eu/en/policies/regulatory-framework-ai

[10] C. Novelli, F. Casolari, A. Rotolo, M. Taddeo, and L. Floridi, "AI Risk Assessment: A Scenario-Based, Proportional Methodology for the AI Act," *DISO*, vol. 3, no. 1, Art. no. 1, May 2024, doi: 10.1007/s44206-024-00095-1.

[11] V. L. Raposo, "Ex machina: preliminary critical assessment of the European Draft Act on artificial intelligence," *International Journal of Law and Information Technology*, vol. 30, no. 1, pp. 88–109, Apr. 2022, doi: 10.1093/ijlit/eaac007.

[12] "The Artificial Intelligence and Data Act (AIDA) – Companion document." [Online]. Available: https://ised-isde.canada.ca/site/innovation-better-canada/en/artificial-intelligence-and-data-act-aida-companion-document

[13] D. Brown, "Canada's Proposed Artificial Intelligence and Data Act (AIDA): A Critical Review," *SSRN Journal*, 2024, doi: 10.2139/ssrn.4687995.

[14] isaperl, "The Canadian Regulation of AI: Focus on the AIDA," Naaia. Accessed: Feb. 06, 2025. [Online]. Available: https://naaia.ai/canadian-regulation-of-ai-focus-on-aida/

[15] J. F. DeFranco and L. Biersmith, "Assessing the State of AI Policy," Jul. 31, 2024, *arXiv*: arXiv:2407.21717. doi: 10.48550/arXiv.2407.21717.

[16] U. Eswaran, V. Eswaran, K. Murali, and V. Eswaran, "Human-Centric AI Balancing Innovation with Ethical Considerations in the Age of Soft Computing," in *Soft Computing in Industry 5.0 for Sustainability*, C. K. K. Reddy, T. Sithole, M. Ouaissa, Ö. Özer, and M. M. Hanafiah, Eds., Cham: Springer Nature Switzerland, 2024, pp. 87–116. doi: 10.1007/978-3-031-69336-6_4.

[17] Dr. A.Shaji George, "India's Ascent as the Global Epicenter of Artificial Intelligence," Feb. 2024, doi: 10.5281/ZENODO.10667648.

[18] E. Choudhary, S. Narayanan, and F. Khan, "Legal and Regulatory Landscape," in *Advances in Healthcare Information Systems and Administration*, B. Singla and K. Shalender, Eds., IGI Global, 2024, pp. 222–239. doi: 10.4018/979-8-3693-7452-8.ch014.

[19] Y. K. Dwivedi *et al.*, "Artificial Intelligence (AI): Multidisciplinary perspectives on emerging challenges, opportunities, and agenda for research, practice and policy," *International Journal of Information Management*, vol. 57, p. 101994, Apr. 2021, doi: 10.1016/j.ijinfomgt.2019.08.002.

[20] R. Belk, "Ethical issues in service robotics and artificial intelligence," *The Service Industries Journal*, vol. 41, no. 13–14, pp. 860–876, Oct. 2021, doi: 10.1080/02642069.2020.1727892.

[21] A. A. Gikay, "Risks, innovation, and adaptability in the UK's incrementalism versus the European Union's comprehensive artificial intelligence regulation," *International Journal of Law and Information Technology*, vol. 32, no. 1, p. eaae013, Jun. 2024, doi: 10.1093/ijlit/eaae013.