European Economic Letters
ISSN 2323-5233
Vol 15, Issue 3 (2025)
http://eelet.org.uk

Artificial intelligence and competition law in india: A legal response to algorithmic market collusions

Sakshi Gupta
Assistant Professor of Law, Maharashtra National Law University, Aurangabad.

Abstract
This article underscores the urgent need for a robust and contemporary legal framework to regulate Artificial Intelligence (AI) in India, particularly through the lens of Competition Law. With AI transforming key sectors like healthcare, finance, and digital services, new challenges are emerging—such as algorithmic collusion, self-preferencing by dominant digital platforms, exploitation of personal data, and the marginalization of smaller market players.

The article critically assesses whether the existing provisions under the Competition Act, 2002 are sufficient to address these AI-driven concerns. It delves into pivotal cases such as Samir Agarwal v. CCI and the Airline Tariff case, which demonstrate the complexities involved in detecting and proving algorithmic collusion. Additionally, the piece explores India's disjointed regulatory landscape, where AI is addressed in fragmented silos—spanning data protection, cyber laws, intellectual property, and sector-specific regulations. The inefficiencies caused by overlapping and missing regulatory elements are brought to light. The article also highlights India's shift from an ex-post to a more proactive ex-ante regulatory approach, exemplified by the proposed Draft Digital Competition Bill based on the recommendations of the Committee on Digital Competition Law (CDCL). By drawing comparative insights from regulatory models in the European Union, United States, and China, the article contextualizes India's regulatory journey on a global scale.

Key policy suggestions include formulating AI-specific competition guidelines, mandating algorithmic transparency, enhancing data-sharing frameworks, and strengthening institutional capacity within the Competition Commission of India (CCI). Ultimately, the article poses a critical question: Can India strike the right balance between regulating AI to ensure fair competition and fostering innovation in a rapidly evolving digital economy?

Keywords: Artificial Intelligence, Data, Algorithm, Competition, Policy.

I. Introduction

The rapid evolution of Artificial Intelligence (AI) has ushered in a new era of technological transformation, fundamentally altering the way businesses operate, compete, and engage with consumers. Encompassing capabilities such as natural language processing, pattern recognition, and autonomous decision-making, AI has enhanced operational efficiency, improved business intelligence, and enabled unprecedented personalization across sectors. However, these advancements raise critical concerns about their impact on market structures and the adequacy of existing regulatory frameworks, particularly competition law.

Competition law, also known as antitrust law seeks to ensure market fairness by preventing monopolistic conduct and anti-competitive practices. Its primary objectives include prohibiting collusive agreements, curbing abuse of dominance, and regulating mergers that

could substantially lessen competition. In India, the Competition Act, 2002, serves as the foundational legal framework in this regard. Yet, this statute was crafted in a pre-AI era, raising pressing questions about its ability to confront the novel challenges posed by algorithm-driven market behavior.

AI introduces complexities unforeseen by traditional legal doctrines. Algorithms can now autonomously adjust prices, monitor competitors, and influence consumer choices without direct human input. Such developments blur the boundaries between independent decision-making and tacit coordination, calling into question the enforceability of existing prohibitions on collusion and dominance. The spectre of algorithmic collusion where software agents converge on pricing strategies absent explicit communication poses a significant threat to market integrity and consumer welfare.

Moreover, the concentration of data, analytics, and computational power in the hands of a few dominant firms has intensified concerns over exclusionary conduct and entry barriers. Companies leveraging AI at scale can reinforce their market positions through predictive analytics, targeted advertising, and real-time responsiveness, advantages that are difficult for smaller competitors to replicate. This may stifle innovation, limit consumer choice, and exacerbate digital inequalities.

AI also enables discriminatory pricing practices based on user behavior and data profiles, potentially leading to unfair or exploitative outcomes. Personalized pricing, while economically efficient, raises ethical concerns and complicates assessments under traditional consumer welfare standards. The opacity of many AI systems, the so-called “black box” problem, further hinders regulatory scrutiny, making it difficult for enforcement agencies to trace accountability or determine the legality of algorithmic outcomes.

In addition, the interaction between AI and intellectual property law creates overlapping challenges. Issues such as data ownership, access to proprietary algorithms, and exclusive licensing can have anti-competitive effects by restricting market entry and knowledge diffusion. These intersections highlight the urgent need for cross-regulatory dialogue and integrated policy frameworks.

Globally, jurisdictions like the European Union have taken proactive steps through initiatives such as the AI Act and the Digital Markets Act, aiming to balance innovation with competition safeguards. In contrast, India’s regulatory approach is still maturing. While the Competition Commission of India (CCI) has begun examining digital markets and algorithmic practices through market studies and consultative processes, a comprehensive legal response remains in development. The proposal of a Digital Competition Bill and the deliberations of the Committee on Digital Competition Law mark important first steps.

This paper explores the evolving interface between AI and competition law in India, identifying emerging risks, enforcement gaps, and opportunities for reform. Through a doctrinal and comparative analysis, it seeks to chart a forward-looking legal framework that is responsive to technological change while grounded in the principles of fair competition.

II. Intersection of ai and competition law

Artificial Intelligence (AI), broadly defined, refers to the simulation of human intelligence by machines, particularly computer systems. According to the *Merriam-Webster Dictionary*[1], AI is "a branch of computer science dealing with the simulation of intelligent behavior in computers," while the *Oxford English Dictionary*[2] describes it as "the study and development of computer systems that can copy intelligent human behaviour." These definitions highlight the core essence of AI: its ability to replicate or simulate cognitive functions such as learning, reasoning, problem-solving, perception, and language understanding.

Interestingly, if one inquires from AI systems themselves about the nature of AI, the response is remarkably consistent. AI is commonly described as a branch of computer science concerned with developing systems capable of performing tasks typically requiring human intelligence. These include decision-making, learning, pattern recognition, language comprehension, and even creative outputs. However, as AI increasingly takes on such roles, particularly in decision-making and market analytics, questions arise regarding the limits of its use, especially in competitive environments.

From the standpoint of competition law, the capabilities of AI present novel and complex challenges. AI-powered pricing algorithms, for example, can inadvertently or intentionally facilitate collusion between competitors by aligning prices through predictive modelling and pattern recognition, even in the absence of explicit agreements. This form of tacit collusion, driven by machine learning, circumvents traditional legal definitions that rely on human communication or intent.

Furthermore, the use of shared AI infrastructure and data pools by multiple firms raises concerns about the indirect exchange of competitively sensitive information. This can reduce the independence of market behavior and contribute to price convergence or market allocation. Dominant firms, equipped with superior data analytics and proprietary AI tools, may exploit these advantages to entrench their market positions through self-preferencing, exclusionary tactics, or personalized pricing strategies that undermine consumer welfare.

These developments complicate the task of regulators, as the opacity of AI systems makes it difficult to detect and prove anti-competitive conduct. Traditional enforcement mechanisms may be ill-equipped to assess algorithmic interactions that produce market distortions without explicit human direction. As a result, jurisdictions worldwide are re-evaluating and modernizing their regulatory toolkits to address AI-driven anti-competitive risks.

In conclusion, while AI holds transformative potential across industries, it also necessitates vigilant oversight to ensure that its deployment does not undermine competition or harm consumers. Legal frameworks, particularly competition law, must evolve in parallel with technology to safeguard market integrity in the digital age.

AI, Algorithms, and the Challenges to Indian Competition Law

[1] *Artificial Intelligence*, Merriam-Webster Dictionary (online), https://www.merriam-webster.com/dictionary/artificial%20intelligence (last visited May 18, 2025).
[2] *Artificial Intelligence*, Oxford English Dictionary (online), https://www.oxfordlearnersdictionaries.com/definition/english/artificial-intelligence (last visited May 18, 2025)

The Competition Act, 2002, serves as the principal legal instrument to curb anti-competitive practices in India by promoting fair competition, protecting consumer interests, and preserving trade freedom. However, the Act was drafted in a pre-digital era and is not fully equipped to address the complexities introduced by Artificial Intelligence (AI). As AI begins to play a determinative role in shaping market behavior often pre-empting human decision-making concerns arise regarding its potential to enable anti-competitive conduct, particularly in the absence of explicit regulatory guidance.

The Competition Commission of India (CCI), while actively engaging with digital markets, faces difficulties in timely detection and disposal of cases involving AI-driven conduct. In this context, the Commission may need to consider sector-specific guidelines or amendments to its enforcement framework to account for algorithmic coordination, data-driven exclusion, and automated pricing strategies.

Understanding Algorithms: From Expert Systems to Learning Machines

Algorithms are sets of rules or procedures followed by machines to solve problems or perform tasks. They vary in complexity based on factors such as the amount of data required, computational power, and the intended application. The simplest type, *expert algorithms* are hard-coded with pre-defined parameters by human developers. These operate with limited flexibility but offer speed and efficiency. More advanced are *learning algorithms*, which can modify or refine their decision parameters based on incoming data. These rely on machine learning (ML) techniques that enable systems to detect patterns, draw inferences, and adapt over time without explicit programming. Such algorithms do not merely execute fixed instructions; they build and evolve decision-making models through continuous interaction with datasets.

These tools have been widely adopted across industries. For instance, airline companies have used algorithmic pricing for decades. Today, similar systems power dynamic pricing in e-commerce, fintech, ride-hailing platforms, and digital insurance markets. As more sectors digitize their operations, the deployment of algorithmic pricing is expanding rapidly.

Software companies now design customized AI tools tailored to the needs of specific firms. Uber's pricing algorithm responds to supply-demand dynamics in real time, while Airbnb's algorithms set differentiated prices based on property characteristics and market signals. These tools not only automate decisions but can also optimize for profit, efficiency, or consumer targeting, depending on the firm's objectives.

The Role of Algorithms in Market Dynamics and Competition Risks

AI-powered algorithms are used in four primary ways that may influence market outcomes and implicate competition law:

1. *Monitoring and Data Collection:* Algorithms enable continuous surveillance of market dynamics, consumer preferences, and competitor behavior. A 2017 European Commission survey found that 78% of surveyed retailers used software tools to monitor competitors' prices. These tools form the backbone of dynamic pricing systems that adjust in response to internal and external variables, such as inventory, demand surges, or rival pricing.

2. *Algorithmic Pricing and Potential for Collusion:* In the e-commerce sector, firms increasingly rely on algorithms to set and adjust prices. When similar or shared algorithms are used across competing firms, there is a risk of parallel pricing behavior or tacit algorithmic collusion. Without human coordination or communication, these algorithms may learn to avoid price wars and sustain supra-competitive pricing, challenging traditional notions of collusion under Section 3 of the Competition Act.

3. *Personalized Targeting and Market Segmentation*: Algorithms can customize product recommendations, advertisements, and offers based on individual user data. These personalization tools rely on large-scale data collection, tracking purchase history, browsing behavior, and user preferences. For instance, consumers frequently observe targeted ads following conversations or searches about specific products, illustrating how consumer data is continuously analyzed and monetized by large platforms.

4. *Data-Driven Consumer Profiling and Behavioral Influence*: Digital platforms collect detailed personal and behavioural data to build profiles that inform pricing, targeting, and service delivery. This profiling enables predictive analytics that may manipulate consumer behavior or result in discriminatory pricing, offering different prices based on perceived willingness to pay. While efficient from a commercial perspective, this raises concerns about consumer autonomy and fairness.

These algorithmic applications pose a serious challenge to regulators. In particular, they raise the question: *Are such practices distorting competition or simply a function of innovation in digital markets?* In India, where there is currently no AI-specific legislation, enforcement remains tethered to conventional competition law principles. Using the term "infringement" in this context may be legally inaccurate as there is no clear statutory basis yet for defining AI-driven practices as violations under the Act.

Moreover, AI-enabled pricing and targeting practices may infringe upon consumer well-being by limiting transparency and choice. For example, a simple Google search for “Hotels in Kasol” may trigger a wave of unsolicited advertisements from various platforms, demonstrating the extent to which consumer data is tracked, processed, and used to influence market behavior. Although privacy issues fall under separate regulatory frameworks, such as the forthcoming Digital Personal Data Protection Act, the overlap between data use and anti-competitive conduct necessitates integrated regulatory thinking.

As algorithms become more central to the business use, regulators are extending their scrutiny beyond the traditional mergers into partnerships, which can also lead to “killer collaborations” between tech giants with AI start-ups. The recent killer collaboration case, involving Amazon's partnership with AI startup anthropic these collaborations raise significant concerns of market dominance by big tech, which leading to the political shift of the competition enforcement from ex post to ex ante. Because of these changes in markets and the growing reliance of shared AI tools, the risk of algorithmic been use in coordinated or collusive way, either intentionally or unintentionally, has increased[3]. However, this use of

[3] Digvijay R. Singh, *Algorithmic Collusion: Can the Competition Act Protect Against Self-Learning Algorithms?*, IndiaCorpLaw Blog (Jan. 6, 2022), https://indiacorplaw.in/2022/01/algorithmic-collusion-can-the-competition-act-protect-against-self-learning-algorithms.html.

algorithms in business conduct can lead to algorithms collusion. there are multiple ways in which algorithms could contribute to human making decision including indirectly. Scholars Ariel Ezrachi and Maurice Stucke describe four main types of algorithmic collusion: messenger, hub-and-spoke, predictable agent and digital eye. [4] The hub-and-spoke method was widely use, and in case of RealPage and Yardi systems, the use of this method was there. The US and EU are taking more initiatives to preventions of algorithmic collusion, and US passed its prevention algorithmic collusion act, 2024.[5] Algorithmic collusion has now been the most significant issue in India in areas such as e-commerce, ride-hailing, and airlines.[6] For example, there are accusations that Ola and Uber companies were involved in price-fixing.[7] In *Samir Agarwal v. Competition Commission of India*, it dismissed claims of the platforms using algorithmic pricing systems for collusion.[8] The Competition Commission of India ('CCI'), however found that there was no evidence of the existence of any such agreement between the platforms. The pricing algorithms used by Ola and Uber are integral to the dynamic pricing models that were used by these companies, which is not part of the explicit collusion agreement.[9] This order has been confirmed by National Company Law Appellate Tribunal ('NCLAT') where it is said that algorithms were devised in response to market conditions and not to serve as anti-competitive means.[10] In the *Airline Tariff Investigation Case in 2014* [11], CCI investigated a price cartel amongst airlines.[12] The airlines made changes in airfares through the third-party algorithms, keeping the seasons, bookings, and other competitor prices in view.[13] Although multiple airlines had followed similar algorithms, there was no specific evidence of a cartel because the final pricing decisions were taken by human persons. Thus, CCI concluded that algorithms had being used for a just price in a highly changing market and did not endorse any kind of unfair practices.[14] Adding to the growing landscape of AI and competition law, the ongoing case *ANI v. OpenAI* [15] involving a prominent Indian news agency accusing OpenAI of unauthorised use of copyrighted content to train ChatGPT and ANI also alleges that AI players like OpenAI using massive data without any permission. Leading to the creation of market barriers for smaller news agencies and content creators for smaller new agencies and content creator. This can lead to abuse of dominant power or unfair business practices. Now the question arises: despite the several judgments, whether the India competition law address algorithmic collusion[16].

---

[4] Ariel Ezrachi & Maurice E. Stucke, *Virtual Competition: The Promise and Perils of the Algorithm-Driven Economy* (Harvard Univ. Press 2019).
[5] S. 3686, 118th Cong. (2024), https://www.congress.gov/bill/118th-congress/senate-bill/3686/text.
[6] Dentons, *supra* note 6.
[7] B. Indulia, *Changing Dynamics of Algorithmic Collusion: An Analytical Study*, SCC Times (May 18, 2023), https://www.scconline.com/blog/post/2023/05/18/changing-dynamics-of-algorithmic-collusion-an-analytical-study/.
[8] *Samir Agrawal v. Competition Commission of India*, 2020 SCC OnLine NCLAT 811.
[9] Id.
[10] Dentons, supra note 6, at 3.
[11] *In re: Alleged Cartelization in the Airlines Industry*, 2021 SCC OnLine CCI 3.
[12]Pricing Algorithms, AZB & Partners (Mar. 15, 2021), https://www.lexology.com/library/detail.aspx?g=80f844ba-f9e1-4bbb-8268-0054179b7ef7.
[13] *In re: Alleged Cartelisation in the Airlines Industry*, *supra* note 14.
[14] *Id.*
[15] *ANI Media Pvt. Ltd. v. OpenAI Inc. & Anr.*, CS(COMM) 1028/2024 (Del. HC Nov. 19, 2024).
[16] *ANI Media Pvt. Ltd. v. OpenAI Inc. & Anr.*, CS(COMM) 1028/2024 (Del. HC Nov. 19, 2024), https://www.nls.ac.in/wp-content/uploads/2024/11/ANI_vs_OPEN_AI.pdf.

Under Section 3 (3) of Indian competition act, 2002[17] deals with collusive agreement between competitors that has AAEC. And this section bans anti-competitive agreements including the action in concert. also, the action in concert covers the informal coordination, like tacit collusion. it was held in the Raghavan committee[18] to identify the cases where companies coordinate secretly. it also points out the oral agreements or informal understanding, they could be considered illegal if they harm the competition. This concept is used in the EU and Us competition law and known as concerted practices. since there are no written evidence, the authorities rely on circumstantial evidence including parallel behaviour and plus factors. [19]

III. Regulatory framework for ai in india

India does not have a dedicated AI regulatory framework. It, instead, has a decentralised regulatory regime where different ministries and sectoral regulators supervise AI-related issues within their jurisdictions.[20] This division of oversight is true to India's approach in addressing the regulatory needs of various industries, each confronted with unique issues of AI integration. Although India does not possess a comprehensive theory of an AI law, it has, however, come to appreciate the need for specific regulations to mitigate the risks posed by technologies with artificial intelligence, especially in the areas of data privacy, security, equity, and ethics.[21]

A. Key legal framework

In the absence of any specific law on AI, its use in India is regulated through various existing laws that were framed to deal with the diverse issues brought about through its use in society.[22] However, the Information Technology Act of 2000 has special importance in the governance of AI activities, especially in matters of cybercrimes and AI-enabled impersonation.[23] Subsection 66D of the Information Technology Act, 2000[24] ('IT Act') renders as illegal the use of systematic computing resources for deceitful criminal activities involving impersonation, which applies to many content fabrics including, but not limited to, deepfakes. Furthermore, privacy and indecent publication offences under section 66E and sections 67A and 67B of the IT Act[25] may also be used against the AI-generated advanced forms of identity theft that violate the privacy and subsequently capture the circulation of harmful content. Furthermore, the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021[26] require intermediaries to control and take down AI content that is privacy invasive or does harm.[27]

---

[17] Competition Act, No. 12 of 2003, § 3(3), *India Code* (2003).
[18]Ministry of Corporate Affairs, *Report of the Competition Law Review Committee* (July 26, 2019), https://www.ies.gov.in/pdfs/Report-Competition-CLRC.pdf.
[19] *Id.*
[20]Shouvik Das, *AI Regulations Will Ideally Be Light Touch, Though Harm Is Concerning*, Mint (Dec. 7, 2023), https://www.livemint.com/news/india/ai-regulations-will-ideally-be-light-touch-though-harm-is-concerning-11701961915125.html (last visited Dec. 22, 2024).
[21] Government of India, *Subcommittee Report on AI Regulation* (Dec. 26, 2023), https://indiaai.s3.ap-south-1.amazonaws.com/docs/subcommittee-report-dec26.pdf.
[22] *Navigating AI in India*, Law. Asia, https://law.asia/navigating-ai-india/.
[23] *Information Technology Act*, No. 21 of 2000, § 66D, *India Code* (2000).
[24] *Id*
[25]*Id.* §§ 66E, 67A, 67B.
[26]Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021 (India).
[27]Government of India, *Subcommittee Report on AI Regulation*, supra note 24.

In the Bharatiya Nyaya Sanhita, 2023 ('BNS') two concerns identified are cheating by impersonation under section 318[28] and defamation by impersonation under section 356[29]. These two concerns completely pertain where an AI system impersonate a person or an AI system generates defamatory statements against a certain individual. At the same time, section 66D of the IT Act and section 67A also consider fraudulent or malicious impersonation, which is particularly relevant to deeper AI impersonations, be it through image or video. Focus and interaction of AI with personal data, privacy and data burden will be covered by the Digital Personal Data Protection Act, 2023 ('DPDP Act') in effect once it comes into force. Relating to Intellectual Property, the even dated Copyright Act, 1957 gives postulations which could concern AI generated works. Section 14(c) of Copyright Act, 1957 provides copyright for works and or database and section 52(1)(a)(i) of Copyright Act, 1957 provides blanket excuses for permission to train an AI system to a point where it uses copyrighted material. Nevertheless assigns few. There are ongoing debates on the best way to make AI systems work within the confines and laws of copyright data specially in commercial value and how to remove the restrictions set towards AI training in data Copyright protection.

To address the shortcomings in the current legal framework, many organizations have pointed out the necessity of incorporating AI governance provisions in the DIA. For example, the Organisation for Economic Co-Operation and Development ('OECD') AI Principles (2019)30 are based on transparency, accountability, and equity in AI systems. Same goes for NITI Aayog's Principles of Responsible AI (2021)31 and NASSCOM Responsible AI Guidelines (2022),[32] which aspires for ethical AI development in India which is in step with international practices.[33] There are no legal framework in place so far to address these concerns, and there is no proposed solution for any of the issues stated. Given the pace at which AI technology is advancing, the policies and laws surrounding it will require constant revisions for the AI systems to be compliant, ethical, and responsible.

B. The role of Competition law in AI regulation

In February 2023, the Ministry of corporate affair (MCA) had constituted committee on digital competition law (CDCL) on the recommendation of 53rd of the parliamentary standing about anti-competitive practices by big tech companies.[34] The committee report on digital competition law identifies the several anti-competitive practices (ACPs), which are usually by the systemically significant digital enterprises (SSDEs). And these ACPs interact with AI driven platform to manipulate the competition. The submission to the committee on digital competition law explained the sharp divide between the regulatory approach. The

---

[28] *Bharatiya Nyaya Sanhita*, No. 45 of 2023, § 318, *India Code* (2023).
[29] *Id.* § 356.
[30] Organisation for Economic Co-operation and Development (OECD), *OECD Principles on Artificial Intelligence* (adopted May 2019, updated July 2024), https://www.oecd.org/en/topics/sub-issues/ai-principles.html.
[31] NITI Aayog, *Operationalizing the Responsible AI Principles* (2021).
[32] NASSCOM, *Responsible AI: Guidelines for Generative AI*, June 2023 ed., https://www.nasscom.in/ai/img/GenAI-Guidelines-June2023.pdf.
[33] Government of India, *Subcommittee Report on AI Regulation*, supra note 24, at 5.
[34] Ministry of Corporate Affairs, Government of India, *Press Release: MCA Invites Public Comments on Report of Committee on Digital Competition Law and Draft Bill on Digital Competition Law*, Press Information Bureau (Mar. 12, 2024), https://pib.gov.in/PressReleasePage.aspx?PRID=2013947.

stakeholder submissions revealed a pattern where supporter of the ex-ante approach include organizations such as the Alliance of Digital India Foundation, all India gaming federation , digital news publishers association , NASSCOM and Paytm and also highlighted the anti-competitive practices such as self-referencing , bundling , anti-steering , unfair commissions by large digital platform for instance the case of *Alphabet Inc. & Ors v. Competition commission of India & Anr.*[35] Conversely, major technology giants like Amazon, Google, Meta, Flipkart and Zomato are not in the favour of ex ante app-arch and raise concerns for ex ante regulatory frameworks for innovation. Whereas AZB & partners and Swiggy proposed a hybrid model based on sector specific assessments. [36]After the considered evaluation the committee on the March 2024, noted that the current ex post framework under the competition act 2002 is not sufficient. The committee recommended enacting the digital competition in an ex ante regulatory framework and released the draft of digital competition bill. [37]

On March 6, 2025, CCI introduced the draft competition commission of India (determination of costs of production) regulations, 2025 .[38] And the consultation was open from February 17, 2025 to March 19, 2025.[39] The draft is not exclusive related to AI, but it targets AI platforms in context of the predatory pricing that is section 4(2)(a)(ii) of competition law of India, 2002[40]. to establish a predatory pricing under section 4(2)(a)(ii) [41], traditionally three elements were required. 1. Dominance, 2. Pricing below cost 3. Intent. traditionally, the intent need to have a proof to eliminate the competition. Which creates a vacuum in the law regarding AI-based pricing. This challenge has been addressed in the draft of competition commission of India (determination of costs of production) regulations, 2025.[42]

C. Evolution of India's AI regulatory approach: Moving towards a risk-based approach.

The country's reluctance to AI regulation by maintaining a pro-innovation position seeking emerging technologies had drastically changed. Similarly, the approach taken in the G20 ministerial meeting and subsequently in Parliament on April 2023 showcased profound abstinence to AI controls.[43] However, since 2022 with advancements being made at the turn

---

[35] *Alphabet Inc. & Ors. v. Competition Commission of India & Anr.*, Competition Appeal (AT) No. 04 of 2023, at ¶ 394 (NCLAT Mar. 28, 2025).
[36] Ministry of Corporate Affairs, Govt. of India, *Report of the Committee on Digital Competition Law*, at 1 (Feb. 27, 2024), https://www.mca.gov.in/bin/dms/getdocument?mds=gzGtvSkE3zIVhAuBe2pbow%253D%253D&type=open.
[37] PRS Legislative Research, *Digital Competition Law*, PRS India (Mar. 12, 2024), https://prsindia.org/policy/report-summaries/digital-competition-law.
[38] Competition Commission of India, *Draft Competition Commission of India (Determination of Cost of Production) Regulations, 2025* (Feb. 17, 2025), https://www.cci.gov.in/images/stakeholderstopicsconsultations/en/draft-competition-commission-of-india-determination-of-cost-of-production-regulations-20251739789121.pdf.
[39] Competition Commission of India, *Stakeholders Topics Consultations*, https://www.cci.gov.in/stakeholders-topics-consultations.
[40] Competition Act, No. 12 of 2003, § 4(2)(a)(ii), *India Code* (2003).
[41] *Id.*
[42] Competition Commission of India, *Draft Cost of Production Regulations, 2025*, supra note 42.
[43] G20 New Delhi Leaders' Declaration (2023), https://www.mea.gov.in/Images/CPV/G20-New-Delhi-Leaders-Declaration.pdf.

of the decade, the country seemed to surprisingly adopt higher level of intrusion, India shifted towards a more interventionist approach.[44]

The shifting India of the 2020s makes it a profoundly interesting case study. In 2023, the Ministry of Electronics and Information Technology (MeitY) implemented the India Digital Act, which showed provisions for controlling the deployment of high-risk Artificial Intelligence systems[45]. These changes signified departure from the 'one size fits all' approach towards AI regulation. Other less traditionally regulated domains like healthcare, financial services and even national security were explicitly stated to be under scrutiny due to the deployment risks of AI in those areas. The AI driven system that could likely result in harm, including deepfake technologies, algorithmic models with biases, amongst others, were rooted as those seeking government attention prior to deployment. This captures one of the key issues of the advisory raised in March 2024 from the Indian government, which focused upon algorithmic models.[46] The advisory was aimed at mitigating risks by attempting to raise barriers focused upon discrimination malpractices, intended to lessen risks of misinformation and discriminatory practices.[47] The tech industry on the other hand lashed out with strong contention resulting in making policy less rigid.[48] This demonstrates how the government is adapting changing their views on AI's regulation from an attempt to solve the negative possibilities of AI towards restriction of AI innovation.[49]

IV. Global approaches to ai regulations: A comparative overview and implications for india

S. no.	Countries	Regulatory Approach

[44] Shaoshan Liu, *India's AI Regulation Dilemma*, The Diplomat (Oct. 27, 2023), https://thediplomat.com/2023/10/indias-ai-regulation-dilemma/.
[45]Ministry of Electronics & Information Technology, Government of India, *Regulation of Hi-Risk AI Systems through Legal, Institutional Quality Testing Framework to Examine Regulatory Models, Algorithmic Accountability, Zero-Day Threat & Vulnerability Assessment, Examine AI-Based Ad-Targeting, Content Moderation etc.*, in *Proposed Digital India Act, 2023* (Mar. 9, 2023), https://www.meity.gov.in/writereaddata/files/DIA_Presentation%2009.03.2023%20Final.pdf.
[46] Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021 (enacted Mar. 1, 2024, revoked Mar. 15, 2024) under Information Technology Act, 2000.
[47] Amlan Mohanty & Shatakratu Sahu, *India's Advance on AI Regulation*, supra note 33, at 7.
[48] Ministry of Electronics & Information Technology, Government of India, *Cyber Law and Data Governance Group, Due Diligence by Intermediaries/Platforms under the Information Technology Act, 2000, and Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021* (Mar. 15, 2024), https://www.meity.gov.in/writereaddata/files/Advisory%2015March%202024.pdf.
[49] Amlan Mohanty & Shatakratu Sahu, *India's Advance on AI Regulation*, supra note 33, at 7.

1.	USA	The regulation of AI stems from Federal Executive Orders on AI safety and ethics, legislation at the state level such as Colorado's risk-based approach and rules regarding algorithmic bias, privacy, and other Ethics & Safety issues. These rules encompass industry specific regulations and those that address entire sectors, including voluntary guidelines set forth by agencies concerning AI safety and security.[50]
2.	CANADA	The AIDA Act in Canada regulates matters of concern in the Canadian ecosystem AI systems which have varying levels of impact on a person or the community at large using a defined tiered risk approach. The Act focuses on protecting human rights, upholding consumer welfare, and ensuring that businesses fulfil their obligations. There are enforced penalties for breaching the regulations, including administrative sanctions as well as criminal prosecution for wilful negligence. As before, this method is participative – it adapts to the pace of economic, social, and technological changes and to international requirements. It focuses on the balanced use of AI technology in areas that provide a risk to public safety and violation of human rights.[51]
3.	AUSTRALIA	Australia has not appointed a dedicated regulatory body for AI, as its AI regulations are voluntary and only guided by the AI Ethics Principles and the Voluntary AI Safety Standard. The government is looking to create AI guardrails for high-risk AI systems, and enforcement will be undertaken by preexisting governing bodies, such as the ACCC and OAIC. These measures will follow an overarching risk-based approach.[52]

[50] *Executive Order on the Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence*, The White House (Oct. 30, 2023), https://www.whitehouse.gov/briefing-room/presidential-actions/2023/10/30/executive-order-on-the-safe-secure-and-trustworthy-development-and-use-of-artificial-intelligence/.
[51] Bill C-27, First Reading, June 16, 2022 (Can.).
[52] *Safe and Responsible AI in Australia*, Department of Industry, Science & Resources, Australian Government (Sept. 2024), https://storage.googleapis.com/converlens-auindustry/industry/p/prj2f6f02ebfe6a8190c7bdc/page/proposals_paper_for_introducing_mandatory_guardrails_for_ai_in_high_risk_settings.pdf.

4.	CHINA	China's Artificial Intelligence Law (Draft) controls the building and application of AI both in China and in any country that affects national security or public interest. It rests upon scientific and technological morality ensuring that the AI development is centered on humans' rights, wellbeing and public health. The draft law features the obligations of the AI developer in the case of negligence, permits copyright uses during model training, and guarantees ownership of inventions made by AI. It also contains instructions to deal with ethical challenges in ensuring AI systems are functional and operative as per the public interest.[53]
5.	SOUTH KOREA	The AI Basic Act which comes into force in January 2026, pertains to high-risk and generative AI. It aims at user safety and transparency, without their stringency being as high as that of the US and EU. The act, for example, mandates firms to inform users about high-risk AI services and impose thorough risk management plans. Failure to comply leads to fines.[54]
6.	EUROPEAN UNION	The EU AI Act recognizes different categories of AI systems according to risk levels, it focuses ai use-specific policieson critical area like healthcare and law enforcement to ensure accountability and trust. Responsibility and reliability are its primary focus. For high-risk applications, safety and transparency is ensured through strict requirements. While the act has binding requirements, co-regulation provisions enable the industry to work with authorities to self-regulate for adherence to laws, ensuring responsible innovation.[55]

[53] Cyberspace Administration of China, National Development & Reform Commission, Ministry of Education, Ministry of Science & Technology, Ministry of Industry & Information Technology, Ministry of Public Security, State Administration of Radio, Film & Television, *Interim Measures for the Management of Generative Artificial Intelligence Services* (enforced Aug. 15, 2023) (China).
[54] *Framework Act on Artificial Intelligence Development and Establishment of a Foundation for Trustworthiness*, Act No. 20676, promulgated Jan. 21, 2025, effective Jan. 22, 2026 (S. Kor.)
[55] *Regulation (EU) 2024/1689 of the European Parliament and of the Council on Artificial Intelligence (EU AI Act)*, [2024] O.J. L1689.

7.	JAPAN	Japan's AI regulations combine emerging statutory frameworks with soft law. Issued by METI in January of 2024, the AI Guidelines for Business outline non-binding etiquette on the ethical and safe employment of AI including the evaluation of the societal impact, safety, and bias prevention measures. Japan has also set out a plan for a more mandatory AI Act in 2025, which targets high-performance AI models. The Act is designed to impose safety systems and compliance reporting, as well as audits and punishments for non-compliance or negligence of global standards such as the EU's AI Act, bridging the gap between the current standards and the needed uptake in AI benefit incorporation.[56]
8.	SINGAPORE	A self-regulatory, sector-specific governance framework which is voluntary and case-specific. A model that helps industries self-regulate with AI use-specific policies and guidelines are available to ensure responsible innovation, development, and deployment.[57]

The regulation of AI within India focuses on three main themes: self-regulation[58], co-regulation[59], and binding rules.[60] Notably, self-regulation is mostly preferred by the industry because it offers a less cumbersome path to compliance and innovation. Existing frameworks proposed by bodies like NITI Aayog and the Indian Council of Medical Research have been successful in more nuanced industries such as digital advertising.[61] The issue is that the vast scope of self-regulation is accompanied by scepticism regarding dealing with public interest. [62] The big argument is that self-regulation allows tech lords to run rampant with their own self-management which completely neglects public interest.[63] It also raises global crises in the US and Singapore, where self-regulation has traditionally been the norm. However, in both countries, this approach has increasingly been countered with greater regulatory

[56] Indian Council of Medical Research, *Guidelines for Application of Artificial Intelligence in Biomedical Research and Healthcare* (2023), https://main.icmr.nic.in/sites/default/files/upload_documents/Ethical_Guidelines_AI_Healthcare_2023.pdf.
[57] InfoComm Media Development Authority & Personal Data Protection Commission Singapore, *Model Artificial Intelligence Governance Framework*, 2d ed. (Jan. 21, 2020), https://www.pdpc.gov.sg/-/media/Files/PDPC/PDF-Files/Resource-for-Organisation/AI/SGModelAIGovFramework2.pdf.
[58] Organisation for Economic Co-operation and Development (OECD), supra note 34, at 6.
[59] Florence G'sell, *Regulating under Uncertainty: Governance Options for Generative AI* (Oct. 6, 2024), https://doi.org/10.2139/ssrn.4918704.
[60] *Regulation (EU) 2024/1689 of the European Parliament and of the Council on Artificial Intelligence (EU AI Act)*, [2024] O.J. L 1689.
[61] NITI Aayog, Government of India, *Responsible AI #AIForAll, Approach Document for India: Part 2 – Operationalizing Principles for Responsible AI* (Aug. 2021).
[62] NASSCOM, supra note 36, at 6.
[63] Interview with an independent lawyer and researcher (Interview no. 14).

inventions.[64] For some, co-regulation is also a plausible method for sectors like high-risk AI applications where public interest is at stake.

Nevertheless, issues from India such as vagueness, lack of general structure, and slow implementation of regulations make them sceptical of adopting set co-regulation for AI without more proof of success in previous noted regions.[65] This can be paralleled with the EU AI Act which supports for high-risk applications through co-regulation albeit with some discussion. Many Indian scholars concur that there is no sufficient thorough risk assessment or discernible market failure; thus, the imposition of binding AI regulations seems unwarranted[66]. Existing laws sufficiently address AI's potential risks, and excessive regulation could hinder innovation. Such a position is identical to the U.S. self-governed approach to AI regulation and Australia's more lenient regulatory approach, which seeks to promote development rather than impose restrictive regulations. Meanwhile, China has championed the cause for stronger high-stakes AI regulation, which is indicative of a governance-centered approach. The approach that India takes towards regulations in Artificial Intelligence still have the opportunities for economic growth and development.[67] India is likely to benefit greatly from AI's impact particularly in its agriculture, healthcare, and finance sectors where Artificial Intelligence is predicted to help boost the Gross Domestic Product (GDP) by 2025.[68] This EU and U.S. approach attempts to make use of AI while dealing with the risks that come with its usage. Cubberley has also argued that uneven resources and low levels of technical understanding disproportionately at the state's disposal created enforcement difficulties. To enable effective enforcement of AI governance, India has to pour funds and strengthen the institutions at the level of AI Safety Institute.[69] In this regard, it would be comparable to EU and U.S. practices which set up institutions to reluctantly cope with headless AI activity and subordinate AI policy enforcement.

India can draw several valuable lessons from international approaches to regulating artificial intelligence (AI) within the realm of competition law. The European Union's AI Act provides a strong example of risk-based regulation, classifying AI systems by their potential impact and imposing strict transparency, accountability, and documentation requirements particularly on high-risk systems like pricing algorithms. This model helps competition authorities detect and address algorithmic collusion and market abuse. In contrast, the United Kingdom adopts a more flexible, sector-specific approach, where the Competition and Markets Authority applies existing laws to AI-related conduct while encouraging innovation. South Korea's AI Basic Act represents an early legal infrastructure aimed at promoting ethical AI development while safeguarding competition. For India, these models highlight the importance of ensuring algorithmic transparency, access to essential data, and coordination between competition law and data protection frameworks. India can also benefit from

[64] Interview with senior Indian government officials involved in AI policy (Interview no. 15 and 16).
[65] Interview with senior law firm partners (Interview no. 11 and 12).
[66] Carnegie Endowment for International Peace, *India's Advance on AI Regulation* (2024), https://carnegieendowment.org/research/2024/11/indias-advance-on-ai-regulation?lang=en&center=india.
[67] Rekha M. Menon, Madhu Vazirani & Pradeep Roy, *Rewire for Success: Boosting India's AIQ*, Accenture (Apr. 26, 2021), https://www.accenture.com/content/dam/accenture/final/a-com-migration/r3-3/pdf/pdf-153/accenture-ai-for-economic-growth-india.pdf.
[68] Press Information Bureau, Government of India, *Press Release* (June 5, 2024), https://pib.gov.in/PressReleasePage.aspx?PRID=2022930
[69] Interview with an executive at an Indian industry body (Interview No. 5); Interview with former Government of India official (Interview No. 7).

investing in regulatory capacity-building, such as establishing specialized AI cells within the Competition Commission of India (CCI). The EU leads globally with the AI Act, the first comprehensive legal framework for AI, effective from August 2024 and phased in through 2026. The Act adopts a risk-based classification of AI systems, unacceptable, high, limited, and minimal risk imposing strict regulations especially on high-risk AI applications that may affect competition, such as those involved in pricing or market allocation. It mandates conformity assessments, risk management, transparency, and accountability, with significant penalties for non-compliance. The Act also establishes governance bodies like the European Artificial Intelligence Board to oversee implementation. The EU competition law addresses AI-enabled anticompetitive behaviors such as algorithmic collusion, cartels, and hub-and-spoke arrangements, emphasizing that while AI can stabilize cartels by automating price coordination, explicit collusion remains illegal. Vertical agreements involving AI, including input foreclosure and resale price maintenance enforced by AI tools, are scrutinized, with hardcore restrictions generally prohibited. Enforcement mechanisms involve both EU and national authorities, requiring enterprises to maintain documentation and ensure AI literacy among employees.

The UK adopts a flexible, sector-specific regulatory model without a standalone AI law. Instead, existing competition and consumer protection laws are applied by regulators like the Competition and Markets Authority (CMA). The CMA actively monitors AI developments, publishes guidance on AI foundation models, and enforces competition law using new powers from the Digital Markets, Competition and Consumers Act. The CMA's principles for AI include open access to inputs, consumer choice, fair dealing, transparency, and accountability, aiming to balance innovation with competition and consumer protection. The UK model empowers sector regulators to oversee AI within their domains rather than imposing a uniform statutory regime.

South Korea enacted the AI Basic Act in December 2024, effective January 2026, positioning itself as the second country with a comprehensive AI legal framework. The Act aims to foster AI innovation while addressing risks related to market concentration and unfair practices, ensuring competitive AI-driven markets and consumer protection. Details on enforcement and specific competition law measures are still developing but align with international trends toward balancing innovation and regulation.

International best practices converge on the need for AI regulatory frameworks that balance innovation with competition safeguards. Key elements include transparency, risk- based regulation, prevention of anticompetitive conduct like algorithmic collusion and input foreclosure, and cooperation among regulators. The EU leads with a comprehensive AI Act integrating competition concerns, the UK relies on sector-specific application of existing laws with proactive regulatory oversight, and South Korea is establishing a foundational AI legal framework to support innovation and fair competition.

V. Challenges

A. Lack of Comprehensive AI-specific legislation

India's AI governing policies are still in its nascent stage and do not have specific, thorough legislations. This gap is filled by relying on existing laws such as the IT Act, BNS or DPDP

Act.[70] These laws are too general and do not provide for the sophisticated matters of AI such as algorithmic accountability, bias detection, or decision-making liability. To some extent, these laws do cover some loopholes, but they do not suitably confront the ex-ante challenges resulting from AI technologies. For example, we see that in the National Strategy for AI (2018), there were set goals such as harnessing the power of AI for healthcare, agriculture, and education. These were all goals, devoid of any guiding principles concerning AI-specific risks.[71] The DPDP Act law has the same focus, while the intent is the specified personal data protection, all other AI issues are vastly unaddressed. [72] This lack of regulating governing concrete dictates results in using a piecemeal approach. Sectoral Regulators such as RBI for perpetration fraud AI and the Medical Council of India for responsible AI in medicine have taken initiative. But still, there is no systematic approach or coordinated-govern structure to tackle a problem of this depth.

B. Gaps in the DPDP Act, 2023

The DPDP Act has made a stride in the legislative framework as it is India's first and most intricate act pertaining to data protection. It helps govern the processing of sensitive personal data and ensures data protection and privacy.[73] The development of Generative AI and Natural Language Processing tools (NLP) depend on vast amounts of publicly accessible information to train their models. However, there are constraints on web scraping or large-scale collection of data.[74] Moreover, Section 3(c)(ii) of the DPDP Act[75] has an exception clause which states that AI firms are allowed to publicly available data such as social media, websites and government records without having to ask for the user's permission. This raises the dilemma: If a person deletes their public information, can AI models continue to use it? Would AI need to cease previously obtained data?[76] Also, Section 17(2)(b) of the DPDP Act[77] states all-encompassing reasons for data processing that are not limited to research and do not require justification are vague and indefinite which assume that any other statistical outline set by the government can be accepted. Once clarifying the problems, where are the defining rules? Who is applicable to this broad coverage? Does it pertain only to academic institutions and universities or do these excuses reach AI companies? The overwhelming amounts of ambiguity induced logic behind defining boundaries about who is entitled to plausibly collect and process the sensitive data such as free access to collecting and conducting research on social experiments and phenomena makes it a problem. Broadening the scope of the exemption makes it easier for both academic institutions and AI enterprises to leverage datasets for machine learning.[78]

---

[70] *Information Technology Act*, No. 21 of 2000, India Code (2000); *Bharatiya Nyaya Sanhita*, 2023, No. 45 of 2023, Gazette of India; *Digital Personal Data Protection Act*, 2023, No. 22 of 2023, Gazette of India.
[71] Government of India, *National Strategy for Artificial Intelligence* (2018).
[72] Government of India, *Subcommittee Report on AI Regulation*, supra note 24, at 5.
[73] *The Digital Personal Data Protection Act, 2023*, No. 22 of 2023, Gazette of India (Aug. 11, 2023), https://www.meity.gov.in/writereaddata/files/Digital%20Personal%20Data%20Protection%20Act%202023.pdf.
[74] Samir Sampat, *Where Do Generative AI Models Source Their Data & Information?*, Smith.ai (Sept. 20, 2023), https://smith.ai/blog/where-do-generative-ai-models-source-their-data-information.
[75] *The Digital Personal Data Protection Act, 2023*, No. 22 of 2023, § 3(c)(ii).
[76] *Five Ways in Which the DPDPA Could Shape the Development of AI in India*, Future of Privacy Forum, https://fpf.org/blog/five-ways-in-which-the-dpdpa-could-shape-the-development-of-ai-in-india/.
[77] *The Digital Personal Data Protection Act, 2023*, No. 22 of 2023, § 17.
[78] Future of Privacy Forum, *supra* note 105.

Nonetheless, without the outlined stringent ethical parameters in place, it results in an absence of privacy where private organisations can exploit personal information for profit motives. Those organizations that operate outside India in relation to offering goods and services to data subjects within India, are covered in section 3(b) of DPDP Act. However, this proviso is narrower in comparison to similar provisions in the Global Data Protections Laws. For example, the GDPR extends to even those corporations which target the data for monitoring purposes. This presents an important gap in regulation that enables foreign AI operators to indiscriminately gather and analyse the sensitive data of Indian citizens without the obstructions posed by the data protection legislation. They can openly monitor Indian users' online activities, scrape social media information, and train AI systems on Indian user data without any hurdles. In contrast, Indian companies miss out on these opportunities.

C. Bias and data discrimination in AI system

The word 'bias' is defined by the international organization for standardization ISO as when the reference value differs from the truth.[79] Applying in context of technology, an AI driven system is deviate in a way that is not neutral or accurate. not all bias inherently considered bad for instance, business like online shopping platforms and streaming services, use AI to make a personalise content for consumers preference based on their implicit bias.[80] While these automated driven AI comes with its challenges. in the academic discourse there are two theories about AI bias that explain the root cause of machine prejudice.[81] the first is the biased training data theory, this theory outlines the gaps in the historical learning and replicate those biases in real world application. and the second theory is biased programmers theory, this theory suggests the AI is biased is influenced by the developer biases intentionally and unintentionally and they become the part of algorithm.[82] additionally this problem can also create when the AI-driven system is designed for something else and used for different context.[83] In some situation the black box become the challenge, in this the lack of transparency makes hinder its ability to identity and rectify the problem.[84] A well-known example of this occurrence is the GPT 4, an advanced linguistic model, a researcher from Stanford found that this language model exhibit strong anti-Muslim bias.[85] This outlines that AI requires a multifaceted approach, which includes better datasets, more diverse team. Completely eliminating entirely bias is impractical, as it often reflects the deep-seated psychological pattern of human in both data and the developer.[86]

---

[79] International Organization for Standardization (ISO), *Statistics—Vocabulary and Symbols—Part 1: General Statistical Terms and Terms Used in Probability* (Sept. 1, 2007), https://www.iso.org/cms/render/live/en/sites/isoorg/contents/data/standard/04/01/40145.html.

[80] S. Milano, M. Taddeo & L. Floridi, Recommender Systems and Their Ethical Challenges, 35 *AI & Society* 957 (2020).

[81] B. Cowgill et al., *Biased Programmers? Or Biased Data? A Field Experiment in Operationalizing AI Ethics* (Dec. 2020), arXiv:2012.02394 [cs, econ, q-fin], http://arxiv.org/abs/2012.02394.

[82] *Id.*

[83] NIST, *NIST Proposes Approach for Reducing Risk of Bias in Artificial Intelligence* (July 13, 2021), https://www.nist.gov/news-events/news/2021/06/nist-proposes-approach-reducing-risk-bias-artificial-intelligence

[84] G. Smith, *UCB Playbook* (2020), https://haas.berkeley.edu/wp-content/uploads/UCB_Playbook_R10_V2_spreads2.pdf.

[85] A. Abid, M. Farooqi & J. Zou, *Large Language Models Associate Muslims with Violence*, 3 Nat. Mach. Intell. 461 (2021).

[86] A. Tversky & D. Kahneman, Judgment under Uncertainty: Heuristics and Biases, 185 *Science* 1124 (1974).

The study conducted by google scholar shows that in India AI driven systems data are western centric which does not fit in the diverse culture of India with population of 1.38 billion people.[87] Since the data is not designed for cater the Indian population so this creates a superficial sense of fairness. Despite India extensively use AI widely for policing[88], facial recognition[89] and healthcare.[90] Majority of the AI research primarily surrounded on racial and gender bias from the western landscape[91] which ignores the axes of injustice against Advasis and Dalits Communities were conveniently left out.[92] For instance, the "aarogya setu", India official virus tracking app excluded millions of poor people who did not have the smartphone raised a question about utility of pan India tracking.[93] Some scholars have observed that India datasets often gets a low quality data treatment in India as well in abroad this leads to data discrimination in India [94] and according to Wallerstein neo liberal AI view Indians as bottom billion data sets. Hence, it is easier for machine learning makers to provide them with poor tech policies or low standards.[95] Another reason also the AI developer is disconnecting with the people for whom the data is made for this gap creates an unfairness in AI system.

D. Intellectual property rights and AI generated content

AI effortlessly and independently generates content, whereas content creation is protected by intellectual property. In India, this is regulated under the Copyright Act, 1957, the Patent Act, 1970, and the Trademark Act, 1999. These existing Intellectual Property ('IP') statutes regarding AI create a gap as they only deal with works produced by humans. Under section 2(d) of the Copyright Act, 1957[96] the law still defines an author to be a natural person only. This poses a gap or ambiguity regarding the copyright of an AI operated system void of human intervention. Here the central problem of authorship occurs: if AI is an not author, who holds the right of the content. This dilemma was brought about in the "DABUS case [97]" of 2021 when an AI called "DABUS" was named an inventor in a patent. The Indian patent office dismissed the claim by stating that under section 2 of the Patents Act, 1970,[98] the author has to be a person. In like manner, the patent law of India raises another issue under Section 52 of the Copyright Act, 1957.[99] Under academic use, the law allows limited use of copyrighted material for self-study or research. On the other hand, there seems to be a

---

[87] N. Sambasivan et al., Re-Imagining Algorithmic Fairness in India and Beyond, in *Proceedings of the 2021 ACM Conference on Fairness, Accountability, and Transparency* (2021).
[88] A. Baxi, *Law Enforcement Agencies in India Are Using Artificial Intelligence to Nab Criminals – Here's How*, Forbes (Sept. 28, 2018), https://www.forbes.com/sites/baxiabhishek/2018/09/28/law-enforcement-agencies-in-india-are-using-artificial-intelligence-to-nab-criminals-heres-how/?sh=548b36eb241d.
[89] P. Dixit, *India Is Creating a National Facial Recognition System, and Critics Are Afraid of What Will Happen Next*, BuzzFeed News (Oct. 10, 2019), https://www.buzzfeednews.com/article/pranavdixit/india-is-creating-a-national-facial-recognition-system-and.
[90] M. Nair, *AI in Healthcare Is India's Trillion-Dollar Opportunity*, World Econ. F. (2022), https://www.weforum.org/agenda/2022/10/ai-in-healthcare-india-trillion-dollar/.
[91] J. Buolamwini & T. Gebru, Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification, in *Proceedings of the 1st Conference on Fairness, Accountability & Transparency*, vol. 81 *Proc. Mach. Learning Rsch.* 77 (PMLR, New York, NY, 2018).
[92] *Id.*
[93] S. Kodali, Aarogya Setu: A Bridge Too Far?, *Deccan Herald* (May 10, 2020), https://www.deccanherald.com/specials/sunday-spotlight/aarogya-setu-a-bridge-too-far-835691.html.
[94] *Id.*
[95] I. Wallerstein, World System versus World-Systems: A Critique, 11 *Critique of Anthropology* 189 (1991).
[96] The Copyright Act, No. 14 of 1957, § 2(d), *India Code* (1957).
[97] *Thaler v. Comptroller-General of Patents, Designs and Trademarks* [2021] EWCA Civ 1374.
[98] The Patents Act, No. 39 of 1970, § 2, *India Code* (1970).
[99] The Copyright Act, No. 14 of 1957, § 52, *India Code* (1957).

blackhole or absence anything that gives power to utilise the copyrighted content for AI model training. Such issues of intellectual property have been presented in the standing committee of calendar year 2021 report number which recommended for updating the intellectual property law of India for making it AI driven.

However, these issues were addressed in the 14 February 2024 by Rajya Sabha members that the existing regulation are adequate for preserving copyright and patent rights in both civil and criminal contexts. They expressed that AI already falls under the regime of copyright protection as provided by the law. It is important to note that IP laws are gradually evolving with the modern advancements surrounding technology.[100] It is no secret that AI has recently taken the world by storm, so the usage of technology and protecting its meta-aspects will continually be a challenging puzzle to solve. It is a common misconception that AI generated content is ambiguously protected under the unreasonable copyright regimes, when no laws currently protect AI generated content. If AI is not a person, how does AI generated content get protected? And if it does, who owns it- the content the programmer produced or the company that hired the programmer? Or if AI generated content is free of copyright, then is it in the public domain and free to use? These questions show the legal gap. This legal gap does not only apply to AI generated content, but ai generated violation of personality rights, which draws attention as to who would be liable when AI imitates human features without permission.[101]

E. Legal personhood and criminal liability of AI

The first critical issue raises surrounding AI and legal personality that whether AI is treated as a legal personhood. In India the legal personhood is define under Article 21 of the constitution. While in the definition the legal personhood status is not restricts to humans, companies are recognised as legal personhood because companies are the stakeholders who hold the accountability. However, AI driven system operates automatically based on its algorithms and machines learning models. Which leads AI to not fit into the definition of legal personhood. Additionally, this raises a concerns of liability when AI causes because the current legal system in India based in the fault an causation concept .According to Andrew D. Selbst, a professor of law at UCLA, they made their observation that the most common use of AI today is in decision assistance to humans rather than fully autonomous robots.[102] For instance, AI in medical diagnosis to analysis the vast amount of data, which takes extensive time for human to notice. Here, AI used as a tool to reduce the workload in the analysis or diagnosis of patient. here AI is used as a tool, not replacing the doctor position of giving the judgment. However, even if the mistake happens in this the doctor is the one who is to be blamed but only to the extend the harm could have been controlled or in the part of the negligence, their liability is not unlimited and if the harm is unexpected they may not be held liable.[103] This happens when the AI works in the complex way which is difficult to interpret

[100] Press Information Bureau, Existing IPR Regime Well-Equipped to Protect AI Generated Works, Government of India (Feb. 9, 2024), https://pib.gov.in/PressReleasePage.aspx?PRID=2004715
[101] *AI and IP: Navigating the Future of Innovation Law*, *Lexology*, https://www.lexology.com/library/detail.aspx?g=da34e703-06a7-4887-9051-55726e21ec54 (last visited Dec. 22, 2024).
[102] Amrita Vasudevan, *Addressing the Liability Gap in AI Accidents*, *Centre for International Governance Innovation* (2023), https://www.jstor.org/stable/resrep52623.
[103] Theodore Porter, *The Rise of Statistical Thinking, 1820–1900* (Princeton Univ. Press 2020), https://www.researchgate.net/publication/348717836_The_Rise_of_Statistical_Thinking_1820-1900.

that is black box[104]. Additionally, the AI often double down on their algorithm by closely guiding the software and data that train their systems.[105] The intractability of AI driven system makes it difficult to predict their actions, which makes liability difficult to establish[106] which corporation Even though, a real-life incident happened related to the fatality caused by a robot (AI) that is the Kenji Urada incident, an engineer in Kawasaki heavy industries, Japan. while repairing the robot, the robot was not switched off and the automated machine detected the engineer as an obstacle or barrier. which pushed me away with causing death of the engineer.

However, without specific AI liability legislation this problem persists. This legal gap creates a subject to legal uncertainty that who holds the accountable in AI involved in criminal activity. According to Hans Kelsens and other scholars the theory of legal personhood is just a technical tool used to provide rights and duties and if AI were recognised as personhood, it would simplify the distribution of liability more efficiently, leading the potential to give a shield to developer and shift the burden of proof to the user. However, many scholars believe that instead of treating AI as an autonomous body, the accountability should be held by the developer or user Because the AI is still evolving. No country has included AI in criminal law till now. and no country in the world has recognised AI as a legal personhood exception is Saudi Arabia which granted citizenship to a Sophia AI in 2017. After this landmark decision the debate was started in the country on whether AI should have. This news sparked a debate in the globe. However, awarding citizenship was just a symbolic gesture, and this raised lot unanswered questions in the globe.[107]

VI. Conclusion

India's Competition Act, 2002, though relatively modern, was designed in an era when digital markets were in their infancy. The exponential rise of digital platforms has disrupted traditional business models and introduced complex competition dynamics. In recognition of these shifts, the Parliamentary Standing Committee on Commerce submitted a landmark report in June 2022 addressing anti-competitive practices by Big Tech firms. This report marked a critical step in India's attempt to develop antitrust tools suited for the digital economy.

This paper evaluates the far-reaching implications of Artificial Intelligence (AI) on Indian competition law. AI technologies particularly those leveraging machine learning, predictive analytics, and data automation have transformed industries by introducing efficiencies and innovation. However, they have also raised serious concerns about fairness, transparency, and market access. The legal frameworks currently in place were not designed to anticipate issues such as algorithmic collusion, self-learning software, and the opacity of automated decision-making.

---

[104] Stela Mecaj, *Artificial Intelligence and Legal Challenges*, 20 Rev. Opinião Jurídica (Fortaleza) 180 (2022), https://www.researchgate.net/publication/360392203_ARTIFICIAL_INTELLIGENCE_AND_LEGAL_CHALLENGES (last visited Mar. 31, 2025).
[105] Jenna Burrell, *How the Machine "Thinks:" Understanding Opacity in Machine Learning Algorithms* (Sept. 15, 2015), https://ssrn.com/abstract=2660674.
[106] Andrew D. Selbst et al., *Fairness and Abstraction in Sociotechnical Systems*, in *Proceedings of the 2019 ACM Conference on Fairness, Accountability, and Transparency* 59 (Aug. 23, 2018), https://ssrn.com/abstract=3265913.
[107] Gali Katznelson, *AI Citizen Sophia and Legal Status*, Petrie-Flom Ctr., Harvard L. Blog (Nov. 2017), https://blog.petrieflom.law.harvard.edu.

A key area of concern is *algorithmic collusion.* Unlike traditional cartels that rely on human coordination, AI systems can learn from competitors' pricing patterns and autonomously arrive at collusive outcomes without explicit communication. This form of tacit coordination challenges conventional antitrust enforcement, which typically requires proof of intent or agreement. As regulators struggle to detect these subtle forms of collusion, dominant firms continue to refine their algorithmic tools, deepening their competitive moat and raising barriers to entry.

Additionally, the *centralization of data and AI capability* within a few dominant players often referred to as "digital gatekeepers" creates serious competition concerns. These firms possess the ability to extract granular insights from consumer data, personalize services, and optimize operations, thereby consolidating market share and excluding smaller players. This cycle of data advantage and market dominance can result in reduced market plurality and stifled innovation.

Another critical issue is *discriminatory pricing*. AI allows firms to segment consumers based on behavior, demographics, and inferred preferences, and set prices accordingly. While such practices enhance profitability and operational efficiency, they may undermine principles of fairness and equal access, particularly when pricing becomes exploitative or opaque. The lack of visibility into algorithmic decision-making commonly referred to as the "black box" problem further complicates regulatory oversight and weakens accountability.

The *intersection of AI, intellectual property (IP), and competition law* adds yet another layer of complexity. Proprietary rights over data, algorithms, and patents can stifle interoperability and prevent competitors from entering or scaling in the market. While IP rights are essential for incentivizing innovation, they can also reinforce anti-competitive conduct when used to deny access to essential AI infrastructure.

While the European Union has made significant strides with the AI Act and the Digital Markets Act, India remains at a formative stage in its regulatory journey. The Competition Commission of India (CCI) has begun to explore AI-related issues through market studies and stakeholder consultations, but a comprehensive legal and institutional response remains pending. The need for clarity on how AI-induced harms will be evaluated under the Competition Act is urgent.

To compound matters, India faces significant structural and strategic deficits in its AI ecosystem. Despite policy efforts such as the *Digital India Act (2023)* and the proposed *IndiaAI Mission*, the country lags behind major economies like China and the United States in AI infrastructure, R&D investment, and strategic autonomy. India's dependence on foreign technology, combined with chronic underinvestment in indigenous AI capabilities, risks relegating the country to a consumer rather than a creator of foundational AI systems.

The brain drain of top AI talent, many of whom lead global innovation but reside outside India further diminishes domestic capacity. Unlike China, which has invested heavily in supercomputing and centralized AI strategies, India's approach has been fragmented and reactive. The National Supercomputing Mission has yet to create AI-specific infrastructure, and major Indian tech companies have largely focused on legacy IT services rather than

disruptive AI R&D[108]. Nevertheless, recent initiatives signal a shift. The *IndiaAI Mission* proposes a ₹10,371 crore (approx. $1.2 billion)[109] investment aimed at boosting AI applications across sectors such as healthcare, agriculture, education, and public services. Early studies also suggest significant potential gains in productivity up to 45% in India's $254-billion IT services sector through the adoption of generative AI technologies[110].

Despite this, India must move beyond isolated programs and adopt a *cohesive, innovation-centric AI policy*. Regulatory responses to AI must not only address market distortions and algorithmic harms but also promote ethical deployment, human oversight, and inclusivity. The lack of investment in culturally rooted projects, such as the underfunded Bhashini initiative, risks ceding India's digital narrative to foreign AI models and undermining linguistic and cultural diversity.

The global economy has witnessed major technological revolutions in energy, telecommunications, and computing but the advent of AI and big data analytics is distinct in both speed and scale. The asymmetry of information between tech giants and regulators, driven by complex machine-learning systems and real-time data processing, has challenged foundational assumptions in antitrust law. As this paper argues, India's legal framework must evolve rapidly to ensure that AI does not undermine fair competition. This involves bridging enforcement gaps, redefining legal standards for AI behavior, and fostering indigenous AI capabilities to ensure regulatory sovereignty. As the country charts its digital future, competition law must remain adaptive, transparent, and aligned with both innovation and public interest.

Suggestions

Given the growing integration of Artificial Intelligence (AI) in digital markets, it is imperative that India's competition law regime evolve to address the emerging risks of algorithmic collusion, data monopolization, and platform self-preferencing. The Competition Commission of India (CCI), as the primary antitrust regulator, must adopt both structural and procedural reforms to keep pace with AI-driven market dynamics. Following suggestions are made in this regard:

1. Sector-Specific Guidelines and Algorithmic Transparency

The CCI should introduce AI-specific guidelines focused on pricing algorithms, automated decision-making, and digital gatekeeping. Disclosure obligations should be made mandatory for dominant players particularly with respect to algorithmic systems that impact pricing, consumer visibility, and market access. Such transparency would foster accountability and help regulators monitor and audit algorithmic behavior more effectively.

2. Ensuring Data Access, Portability, and Interoperability

---

[108] *China Daily HK Article*, *China Daily HK*, https://www.chinadailyhk.com/hk/article/604172.

[109] *India to Invest Rs 10,372 Crore in AI Infrastructure, Startups for Five Years*, *The New Indian Express* (Mar. 8, 2024), https://www.newindianexpress.com/business/2024/Mar/08/india-to-invest-rs-10372-crore-in-ai-infrastructure-startups-for-five-years.

[110] *GenAI to Boost India's IT Industry Productivity by 45%, EY India Survey Shows*, *Channel News Asia*, https://www.channelnewsasia.com/business/genai-boost-indias-it-industrys-productivity-up-45-ey-india-survey-shows-4928186.

With the Digital Personal Data Protection Act (DPDP) still in its early stages, India lacks a mature framework for addressing data-driven exclusion. Competition law must step in to ensure fair access to both personal and non-personal datasets held by dominant entities. Data portability and interoperability mandates can help lower entry barriers for startups and SMEs, thereby promoting innovation and inclusivity.

3. Embracing an Ex-Ante Regulatory Model
India's proposed Digital Competition Act, as envisioned by the Committee on Digital Competition Law (CDCL), marks a significant shift from an ex-post to an ex-ante enforcement paradigm. Inspired by the European Union's Digital Markets Act, this proactive approach would allow the CCI to intervene before harm occurs crucial in fast-moving digital markets where traditional remedies often arrive too late to be effective.

4. Establishment of a Specialized Technical Committee within CCI
The CCI must set up a dedicated Technical Committee composed of experts in AI, data science, and algorithmic markets. This body would serve as a techno-legal bridge analyzing AI systems used by firms, identifying potential anti-competitive patterns, and advising on enforcement strategy. Such specialization is essential for tackling opaque and self-learning algorithmic systems.

5. Cross-Border Collaboration for Harmonized Regulation
Given the global nature of AI and digital commerce, India should engage in structured dialogue with international competition regulators. Collaboration on enforcement strategies, research initiatives, and standard-setting would enhance India's influence in global digital governance and reduce regulatory fragmentation for multinational firms.

6. Mandatory Algorithmic Audits and Penalty Regime
Enterprises deploying AI systems should be subject to annual algorithmic audits to assess compliance with competition laws, transparency obligations, and ethical norms. Non-compliance should attract significant monetary penalties potentially up to 1% of global turnover ensuring strong deterrence against collusive or exclusionary algorithmic conduct.

7. Development of AI-Based Detection Tools
The CCI must invest in the creation or acquisition of advanced AI tools to proactively detect algorithmic collusion. Such tools can use behavioral screens, data mining, and anomaly detection to flag suspicious market behavior. Pattern recognition systems would allow for timely interventions, minimizing consumer harm and increasing regulatory efficiency.

8. Institutional Collaboration with MeitY
A joint regulatory strategy between the CCI and the Ministry of Electronics and Information Technology (MeitY) is critical. This would align competition law enforcement with broader AI governance policies, including those pertaining to cybersecurity, data ethics, and digital trust. Regulatory coherence will reduce overlaps and strengthen India's overall digital policy architecture.

9. Enhanced Advocacy and Awareness
The CCI should expand its advocacy efforts to raise awareness among firms, consumers, and developers about AI-related competition risks. Publicizing enforcement outcomes,

conducting training workshops, and issuing guidance documents would promote a culture of compliance and ethical algorithmic development.

10. Stronger Penalties for AI-Enabled Cartels

Given the sophisticated nature and significant harm potential of AI-facilitated collusion, India should adopt a differentiated penalty regime. Fines for such behavior should be significantly higher than those for traditional cartels, reflecting the heightened complexity and difficulty of detection.

11. Deployment of Market Behavior Screens

The CCI could leverage AI to implement behavioural conduct screens that flag unusual market conduct suggestive of collusion. These systems would track pricing patterns, input-cost changes, and firm responses over time to detect "structural breaks" indicative of coordinated behavior. Big data analytics can turn this from theory into practice, enabling more accurate investigations.

12. Creation of a Dedicated Tribunal for AI and Digital Market Disputes

Given the interdisciplinary nature of AI-related cases, India should establish a Specialized Technical Tribunal for digital and AI disputes. This tribunal would consist of legal professionals and technical experts to ensure nuanced adjudication. Such a forum would speed up case resolution, improve decision quality, and address the growing knowledge gap between law and technology.

As India positions itself as a digital leader, it must develop a robust, innovation-friendly legal framework that ensures fair competition in AI-enabled markets. The unique challenges of algorithmic opacity, data dominance, and automated decision-making call for targeted reforms in law, policy, and institutional design. India must learn from global best practices while crafting solutions grounded in its domestic realities. A collaborative model anchored in regulatory agility, technological expertise, and stakeholder engagement will be key to building a competitive, inclusive, and ethical AI economy.