



International Journal of Research Publication and Reviews

Journal Homepage: www.ijrpr.com ISSN 2582-7421

AI Agents as Autonomous Economic Actors: Who Bears Competition-Law Liability When an AI Agent Negotiates, Prices or Purchases on Behalf of a Firm?

Aditya Mishra, Ankul Prajapati, & Md Saqib Ansari

National Law Institute University, Bhopal, Madhya Pradesh 462044, India

ABSTRACT

Autonomous AI agents increasingly negotiate, price and purchase on behalf of firms, yet competition law attributes conduct to humans and enterprises through doctrines of agreement, intent and concerted action. This paper examines the attribution gap that arises when self learning agents produce commercially significant, potentially anti competitive outcomes without clear human consensus. Focusing on the Competition Act, 2002, it argues that liability should remain with the deploying firm under an enterprise risk model, supplemented by a Control, Authorisation, Duty, Causation and Rule (CADCR) test to allocate responsibility across developers, vendors and beneficiaries where autonomy is high. Doctrinal analysis shows that Sections 2(b) and 3 can cover many AI mediated scenarios, especially in hub and spoke or common platform cases, but purely autonomous convergence strains the “meeting of minds” paradigm. Drawing on global enforcement trends in the United States, European Union, United Kingdom and Brazil, the paper proposes de lege ferenda reforms, including a targeted provision prohibiting algorithmic pricing systems that cause appreciable adverse effects, with rebuttable presumptions and disclosure powers. A compliance architecture is outlined, emphasising governance, algorithmic audits, data segregation and evidence preservation. The paper concludes that autonomy redistributes but does not eliminate accountability, and that Indian competition law should evolve from a purely consensus based model to an attribution framework tied to control, foreseeability and enterprise benefit.

Keywords: AI agents; competition law; algorithmic pricing; attribution of liability; enterprise risk; hub and spoke; Competition Act, 2002; CADCR test.

I. Introduction

Artificial intelligence has moved from passive analytics to active commercial agency. Modern AI agents do not merely recommend prices or flag anomalies; they perceive market data, set objectives such as margin maximisation, and execute transactions including quoting, negotiating and purchasing with limited human intervention.¹ This shift from tool to agent places competition law under stress because its core doctrines attribute conduct to firms and individuals through concepts of agreement, decision and concerted action that presuppose human agency and intent.² When an AI agent independently negotiates terms, aligns prices with rivals, or selects suppliers, the question is no longer only whether the outcome harms competition, but who bears liability for that outcome under the Competition Act, 2002.³

Indian competition law is built on an enterprise model. Section 2(b) defines “agreement” broadly to include any arrangement, understanding or action in concert, while Section 3(1) prohibits agreements that cause or are likely to cause an appreciable adverse effect on competition.⁴ Section 3(3) creates presumptions for horizontal practices such as price fixing, and Section 4 addresses abuse of dominance without requiring an agreement.⁵ Yet these

¹ See Trmlabs, Autonomous AI Agents and Financial Crime: Risk, Responsibility and Accountability (Feb. 26, 2026), <https://www.trmlabs.com/resources/blog/autonomous-ai-agents-and-financial-crime-risk-responsibility-and-accountability>; see also Scholar Club, Attributing Legal Liability for Autonomous AI Agents in Crypto Asset Markets, J. L. & Soc. Sci. (Aug. 11, 2026), <https://scholarclub.org/index.php/jllsa/article/view/249>.

² Competition Act, 2002, § 2(b), § 3(1) (India); see also LiveLaw, Jurisprudential Dilemma of Algorithmic Cartels (Apr. 17, 2026), <https://www.livelaw.in/articles/jurisprudential-dilemma-algorithmic-cartels-530685>.

³ Competition Act, 2002, § 3(1), § 4 (India); see also Bar & Bench, Beyond the Agreement Paradigm: Regulating Algorithmic Collusion under the Competition Act, 2002 (June 30, 2026), <https://www.barandbench.com/columns/beyond-the-agreement-paradigm-regulating-algorithmic-collusion-under-the-competition-act-2002>.

⁴ Competition Act, 2002, § 2(b), § 3(1) (India); see also K SandK, Algorithmic Collusion and Section 3(3) Competition Act (Mar. 2, 2026), <https://ksandk.com/competition/algorithmic-collusion-competition-act/>.

⁵ Competition Act, 2002, § 3(3), § 4 (India); see also K SandK, Indian Competition Law — Complete Guide (Feb. 24, 2026), <https://ksandk.com/competition-review/guides/indian-competition-law/>.

provisions were drafted for human wrongs in markets and assume a meeting of minds or at least conscious parallelism supported by plus factors.⁶ Self learning pricing agents can produce sustained coordination without communication, shared platforms or explicit design for alignment, thereby creating an attribution gap between harmful effects and provable consensus.⁷

This paper argues that liability should remain with the deploying firm under an enterprise risk and attribution framework, supplemented by a control, authorisation, duty, causation and rule test to allocate responsibility across developers, operators and beneficiaries where autonomy is high.⁸ The thesis rests on three premises. First, AI agents lack legal personhood and cannot be sanctioned; responsibility must rest with the humans and entities that design, deploy, authorise or benefit from the system.⁹ Second, global enforcement signals that the use of an algorithm or agent is not a defence, and liability can attach to deployment choices, data flows and oversight failures even where intent is opaque.¹⁰ Third, India can leverage its broad “agreement” language to cover many AI mediated scenarios, but may need targeted presumptions and disclosure powers for high risk algorithmic pricing to avoid under enforcement or over deterrence.¹¹

The analysis proceeds in three steps. It maps the typology of algorithmic and agentic conduct relevant to competition law and explains why autonomy matters for attribution.¹² It then undertakes a doctrinal reading of Sections 2(b), 3 and 4 of the Competition Act, 2002 in light of recent CCI market studies and global enforcement trends on algorithmic pricing.¹³ Finally, it proposes a compliance oriented attribution framework for adjudicators and a governance architecture for firms, with a view to preserving deterrence while accommodating innovation in commercial AI.¹⁴

II. Conceptual Foundations: AI Agents in Commercial Decision-Making

2.1 Typology of algorithmic conduct relevant to competition law

Algorithmic conduct in markets can be classified into four functional types, each carrying distinct antitrust risk and doctrinal characterisation under the Competition Act, 2002. First, monitoring algorithms are used to detect and punish deviations from a human devised cartel, thereby stabilising collusion.¹⁵ These are most readily characterised as “agreement” or “action in concert” under Section 2(b) read with Section 3(1), because they implement and enforce a pre existing consensus among rivals.¹⁶ Second, parallel or hub and spoke algorithms operate through shared pricing platforms or common vendors, enabling competitors to align prices without direct communication.¹⁷ Indian authorities and scholars increasingly treat such scenarios as “arrangement” or “understanding” where the hub facilitates interdependence and the spokes knowingly adopt the system.¹⁸ Third, signalling algorithms react in real time to rivals’ public moves, producing reactive alignment that may amount to concerted practice if coupled with plus factors such as sustained parallelism and market structure conducive to coordination.¹⁹ Fourth, self learning algorithms, including reinforcement learning agents, can discover coordination

⁶ LiveLaw, supra note 2; see also CBCL NLIU, Addressing Algorithmic Collusion in Indian Competition Law (Dec. 16, 2025), <https://cbcl.nliu.ac.in/competition-law/addressing-algorithmic-collusion-in-indian-competition-law/>.

⁷ Bar & Bench, supra note 3; see also IRCCL, Algorithmic Collusion and the Limits of Agreement under Indian Competition Law (Feb. 20, 2026), <https://www.irccl.in/post/algorithmic-collusion-and-the-limits-of-agreement-under-indian-competition-law>.

⁸ Scholar Club, supra note 1; Trmlabs, supra note 1.

⁹ Trmlabs, supra note 1; see also Digital L. J., Artificial Intelligence and Liability: Exploring Legal Challenges and Responsibility in AI Decision Making and Autonomous Systems (June 5, 2026), <https://www.digitallawjournal.org/jour/article/view/320>.

¹⁰ Reuters, Collusion by Code? Understanding Algorithmic Pricing and Antitrust Enforcement (Mar. 20, 2026), <https://www.reuters.com/legal/legalindustry/collusion-by-code-understanding-algorithmic-pricing-and-antitrust-enforcement-pracin-2026-03-20/>; see also Akin Gump, CMA Highlights Real World Risks of Algorithmic Pricing (Mar. 16, 2026), <https://www.akingump.com/en/insights/alerts/when-bots-set-prices-cma-highlights-real-world-risks-of-algorithmic-pricing>.

¹¹ Bar & Bench, supra note 3; see also Noah News, India Considers New Legal Framework to Address Algorithmic Collusion Risks (June 30, 2026), <https://noah-news.com/india-considers-new-legal-framework-to-address-algorithmic-collusion-risks/>.

¹² CBCL NLIU, supra note 6; see also CICTL, Invisible Cartels in Digital Markets: Algorithmic Pricing and the Limits of Competition Law (June 7, 2026), <https://www.cictl.in/post/invisible-cartels-in-digital-markets-algorithmic-pricing-and-the-limits-of-competition-law-1>.

¹³ Competition Act, 2002, § 2(b), § 3, § 4 (India); see also K SandK, supra note 5.

¹⁴ Trmlabs, supra note 1; see also Reuters, supra note 10.

¹⁵ CBCL NLIU, Addressing Algorithmic Collusion in Indian Competition Law (Dec. 16, 2025), <https://cbcl.nliu.ac.in/competition-law/addressing-algorithmic-collusion-in-indian-competition-law/>.

¹⁶ Competition Act, 2002, § 2(b), § 3(1) (India); see also LiveLaw, Jurisprudential Dilemma of Algorithmic Cartels (Apr. 17, 2026), <https://www.livelaw.in/articles/jurisprudential-dilemma-algorithmic-cartels-530685>.

¹⁷ CBCL NLIU, supra note 1; see also CICTL, Invisible Cartels in Digital Markets: Algorithmic Pricing and the Limits of Competition Law (June 7, 2026), <https://www.cictl.in/post/invisible-cartels-in-digital-markets-algorithmic-pricing-and-the-limits-of-competition-law-1>.

¹⁸ K SandK, Algorithmic Collusion and Section 3(3) Competition Act (Mar. 2, 2026), <https://ksandk.com/competition/algorithmic-collusion-competition-act/>; see also Bar & Bench, Beyond the Agreement Paradigm: Regulating Algorithmic Collusion under the Competition Act, 2002 (June 30, 2026), <https://www.barandbench.com/columns/beyond-the-agreement-paradigm-regulating-algorithmic-collusion-under-the-competition-act-2002>.

¹⁹ IRCCL, Algorithmic Collusion and the Limits of Agreement under Indian Competition Law (Feb. 20, 2026), <https://www.irccl.in/post/algorithmic-collusion-and-the-limits-of-agreement-under-indian-competition-law>.

strategies autonomously, without explicit design for alignment.²⁰ These pose the hardest doctrinal fit, because outcomes may resemble collusion while lacking a provable meeting of minds, pushing analysis toward effects based readings of Section 3(1) or, *de lege ferenda*, a targeted algorithmic pricing rule.²¹

2.2 Autonomy spectrum and legal relevance

The legal relevance of algorithmic conduct turns on the degree of autonomy. Low autonomy systems, such as rule based pricing engines that apply human set formulas within fixed bands, permit relatively straightforward attribution to firm intent.²² Courts and enforcers can infer that the firm authorised the pricing logic and accepted its market effects, satisfying the consensus or conscious parallelism requirements under Section 3.²³ By contrast, high autonomy agents learn from market feedback, adjust objectives and can initiate transactions without real time human approval.²⁴ In such cases, intent and knowledge become opaque, and the “meeting of minds” assumption underlying agreement based liability grows tenuous.²⁵ This autonomy spectrum therefore maps onto an attribution gap: as agents acquire discretion to negotiate, price and purchase, the link between human authorisation and anti competitive outcome weakens, raising questions of foreseeability, duty of oversight and enterprise risk.²⁶

2.3 Why “agent” matters (not just “algorithm”)

The shift from algorithm to agent is legally material because agents perform functions traditionally carried out by authorised employees or legal agents. They can perceive market conditions, select counterparties, negotiate terms and execute purchases on behalf of the firm.²⁷ This triggers agency law analogies alongside competition law attribution. Concepts such as scope of authority, actual and apparent authorisation, and ratification become relevant to determine whether the firm is bound by the agent’s commercial acts.²⁸ Where an AI agent operates within pre approved parameters and the firm benefits from its outcomes, competition authorities can treat the agent’s conduct as the firm’s conduct for purposes of Sections 3 and 4.²⁹ At the same time, the capacity of agents to act across firm boundaries through shared platforms or data feeds revives hub and spoke theories, making vendor and platform liability a live issue where design or data flows facilitate coordination.³⁰

III. The Attribution Gap in Competition Law

3.1 Enterprise liability and the “agreement” paradigm

Indian competition law rests on an enterprise liability model. Section 3(1) of the Competition Act, 2002 prohibits any agreement that causes or is likely to cause an appreciable adverse effect on competition, while Section 2(b) defines “agreement” expansively to include any arrangement, understanding or action in concert.³¹ This breadth allows authorities to capture informal consensus and coordinated conduct without a formal contract, and to treat sustained parallel behaviour plus plus factors as evidence of an understanding.³² The paradigm, however, presumes human agency. It assumes that firms or

²⁰ CBCL NLIU, *supra* note 1; see also LiveLaw, Coded Collusion: Algorithmic Pricing in Indian Aviation and Structural Failure of Competition Law (June 9, 2026), <https://www.livelaw.in/articles/algorithmic-pricing-indian-aviation-structural-failure-competition-law-537241>.

²¹ Bar & Bench, *supra* note 4; see also Noah News, India Considers New Legal Framework to Address Algorithmic Collusion Risks (June 30, 2026), <https://noah-news.com/india-considers-new-legal-framework-to-address-algorithmic-collusion-risks/>.

²² JD Supra, Algorithmic Pricing and AI Powered Evidence Avoidance (Mar. 27, 2026), <https://www.jdsupra.com/legalnews/algorithmic-pricing-and-ai-powered-1056402/>.

²³ K SandK, *supra* note 4; see also Competition Act, 2002, § 3(1), § 3(3) (India).

²⁴ LiveLaw, *supra* note 2; see also CBCL NLIU, *supra* note 1.

²⁵ LiveLaw, *supra* note 6; see also IRCCL, *supra* note 5.

²⁶ Trmlabs, Autonomous AI Agents and Financial Crime: Risk, Responsibility and Accountability (Feb. 26, 2026), <https://www.trmlabs.com/resources/blog/autonomous-ai-agents-and-financial-crime-risk-responsibility-and-accountability>; see also Scholar Club, Attributing Legal Liability for Autonomous AI Agents in Crypto Asset Markets, J. L. & Soc. Sci. (Aug. 11, 2026), <https://scholarclub.org/index.php/jllsa/article/view/249>.

²⁷ IMDA, Legal Responsibility for AI Agents (May 21, 2026), <https://www.imda.gov.sg/-/media/imda/files/about/emerging-tech-and-research/artificial-intelligence/agents-legal-responsibility.pdf>.

²⁸ *Id.*

²⁹ Competition Act, 2002, § 2(b), § 3(1), § 4 (India); see also K SandK, Indian Competition Law — Complete Guide (Feb. 24, 2026), <https://ksandk.com/competition-review/guides/indian-competition-law/>.

³⁰ Reuters, Collusion by Code? Understanding Algorithmic Pricing and Antitrust Enforcement (Mar. 20, 2026), <https://www.reuters.com/legal/legalindustry/collusion-by-code-understanding-algorithmic-pricing-and-antitrust-enforcement--pracin-2026-03-20/>; see also Akin Gump, CMA Highlights Real World Risks of Algorithmic Pricing (Mar. 16, 2026), <https://www.akingump.com/en/insights/alerts/when-bots-set-prices-cma-highlights-real-world-risks-of-algorithmic-pricing>.

³¹ Competition Act, 2002, § 2(b), § 3(1) (India); see also LiveLaw, Jurisprudential Dilemma of Algorithmic Cartels (Apr. 17, 2026), <https://www.livelaw.in/articles/jurisprudential-dilemma-algorithmic-cartels-530685>.

³² K SandK, Algorithmic Collusion and Section 3(3) Competition Act (Mar. 2, 2026), <https://ksandk.com/competition/algorithmic-collusion-competition-act/>; see also Bar & Bench, Beyond the Agreement Paradigm: Regulating Algorithmic Collusion under the Competition Act, 2002 (June

individuals consciously choose to align conduct, communicate directly or through intermediaries, or at least knowingly adopt a common course that produces anti competitive effects.³³

Self learning AI agents stress this assumption. Such agents can observe market data, adjust pricing or procurement strategies through reinforcement learning, and converge on coordinated outcomes without explicit communication, shared platforms or design level collusion.³⁴ In these scenarios, there may be no human “smoking gun” and no conscious parallelism in the traditional sense, yet the market effect resembles a cartel.³⁵ The result is an attribution gap between harmful outcomes and the doctrinal requirements of agreement or concerted action under Sections 2(b) and 3(1).³⁶ Indian scholarship notes that while simple algorithms implementing human devised cartels fit comfortably within the agreement paradigm, autonomous coordination by learning agents exposes the limits of a meeting of minds test.³⁷

3.2 Intent, knowledge, and foreseeability

Traditional enforcement under Section 3 leans on proof of consensus or, failing that, conscious parallelism supported by plus factors such as market concentration, transparency and sustained uniformity.³⁸ Intent or knowledge is often inferred from conduct, communications and structural conditions.³⁹ With AI agents, firms can argue that they lacked knowledge of the specific pricing decisions, did not intend coordination, and could not foresee the emergent behaviour of a self learning system.⁴⁰ Global enforcement trends, however, signal that the use of an algorithm or agent is not a defence. Authorities in the United States, European Union, United Kingdom and Brazil have pursued cases where liability attaches to deployment choices, data flows and oversight failures, even where the precise decision path of the algorithm is opaque.⁴¹ The emerging principle is that firms cannot outsource compliance to code. Continued deployment of a pricing or procurement agent in the face of foreseeable anti competitive effects can itself be treated as fault, shifting analysis from subjective intent to enterprise risk and duty of care.⁴²

3.3 The “double opacity” problem

AI mediated markets suffer from a double opacity. Algorithmic opacity refers to the difficulty of explaining how a model reaches a particular decision, especially in deep learning or reinforcement learning systems.⁴³ Transactional opacity refers to the difficulty of tracing who authorised, benefited from or could have intervened in a specific commercial act executed by an agent across complex organisational and vendor ecosystems.⁴⁴ Together, these opacities complicate the allocation of responsibility among developers, deployers, infrastructure providers and beneficiaries.⁴⁵ A developer may claim that the firm misused the tool, the firm may claim that the vendor designed for alignment, and both may point to market forces as the true cause.⁴⁶

This creates two enforcement risks. First, under enforcement arises when authorities cannot identify a human actor with sufficient knowledge or intent, allowing harmful coordination to escape liability.⁴⁷ Second, over deterrence arises if firms are penalised for unpredictable outputs despite robust

30, 2026), <https://www.barandbench.com/columns/beyond-the-agreement-paradigm-regulating-algorithmic-collusion-under-the-competition-act-2002>.

³³ LiveLaw, supra note 1; see also CBCL NLIU, Addressing Algorithmic Collusion in Indian Competition Law (Dec. 16, 2025),

<https://cbcl.nliu.ac.in/competition-law/addressing-algorithmic-collusion-in-indian-competition-law/>.

³⁴ LiveLaw, Coded Collusion: Algorithmic Pricing in Indian Aviation and Structural Failure of Competition Law (June 9, 2026),

<https://www.livelaw.in/articles/algorithmic-pricing-indian-aviation-structural-failure-competition-law-537241>; see also IRCCL, Algorithmic Collusion and the Limits of Agreement under Indian Competition Law (Feb. 20, 2026), <https://www.irccl.in/post/algorithmic-collusion-and-the-limits-of-agreement-under-indian-competition-law>.

³⁵ Bar & Bench, supra note 2; see also Noah News, India Considers New Legal Framework to Address Algorithmic Collusion Risks (June 30, 2026),

<https://noah-news.com/india-considers-new-legal-framework-to-address-algorithmic-collusion-risks/>.

³⁶ Competition Act, 2002, § 2(b), § 3(1) (India); see also LiveLaw, supra note 1.

³⁷ CBCL NLIU, supra note 3; see also IRCCL, supra note 4.

³⁸ K SandK, supra note 2; see also LiveLaw, supra note 1.

³⁹ K SandK, supra note 2.

⁴⁰ CBCL NLIU, supra note 3; see also LiveLaw, supra note 4.

⁴¹ HLC, Update on Algorithmic Pricing in Competition Law (Oct. 14, 2025), <https://www.hlc.com/en/publications/update-on-algorithmic-pricing-in-competition-law-what-you-need-to-know>; see also Akin Gump, CMA Highlights Real World Risks of Algorithmic Pricing (Mar. 16, 2026), <https://www.akingump.com/en/insights/alerts/when-bots-set-prices-cma-highlights-real-world-risks-of-algorithmic-pricing>.

⁴² HLC, supra note 11; see also Reuters, Collusion by Code? Understanding Algorithmic Pricing and Antitrust Enforcement (Mar. 20, 2026), <https://www.reuters.com/legal/legalindustry/collusion-by-code-understanding-algorithmic-pricing-and-antitrust-enforcement-pracin-2026-03-20/>.

⁴³ Trmlabs, Autonomous AI Agents and Financial Crime: Risk, Responsibility and Accountability (Feb. 26, 2026),

<https://www.trmlabs.com/resources/blog/autonomous-ai-agents-and-financial-crime-risk-responsibility-and-accountability>.

⁴⁴ Id.; see also Scholar Club, Attributing Legal Liability for Autonomous AI Agents in Crypto Asset Markets, J. L. & Soc. Sci. (Aug. 11, 2026), <https://scholarclub.org/index.php/jllsa/article/view/249>.

⁴⁵ Trmlabs, supra note 13.

⁴⁶ Id.; see also Digital L. J., Artificial Intelligence and Liability: Exploring Legal Challenges and Responsibility in AI Decision Making and Autonomous Systems (June 5, 2026), <https://www.digitallawjournal.org/jour/article/view/320>.

⁴⁷ CBCL NLIU, supra note 3; see also LiveLaw, supra note 4.

governance, chilling beneficial innovation in pricing and procurement AI.⁴⁸ The doctrinal challenge is therefore to construct an attribution framework that preserves deterrence by tying liability to control, authorisation and foreseeable effects, while avoiding strict liability for truly unforeseeable machine behaviour.⁴⁹

IV. Doctrinal Analysis under the Competition Act, 2002

4.1 Section 2(b): Can “action in concert” capture AI-mediated coordination?

Section 2(b) of the Competition Act, 2002 defines “agreement” to include any arrangement, understanding or action in concert.⁵⁰ This purposive definition enables the Competition Commission of India to look beyond formal contracts and capture informal consensus and coordinated conduct that produces anti competitive effects.⁵¹ In AI mediated markets, “action in concert” can be read to cover technologically mediated interdependence where competitors knowingly adopt similar pricing or procurement systems, share data feeds or use common platforms that structurally predispose them to aligned outcomes.⁵² Indian scholarship supports this view, arguing that sustained parallelism facilitated by shared algorithms or hubs can be treated as an “understanding” or “arrangement” even without explicit communication.⁵³

However, there is a limit. Purely autonomous convergence, where self learning agents independently discover coordination without design level collusion, shared platforms or common data sources, may fall outside the ordinary meaning of “arrangement” or “understanding”.⁵⁴ In such cases, there is no human consensus to adopt a common course, and the coordination emerges from machine learning rather than concerted choice.⁵⁵ This exposes a doctrinal gap: harmful effects exist, but the agreement element under Section 2(b) read with Section 3(1) is difficult to establish without stretching the concept of action in concert beyond recognition.⁵⁶

4.2 Section 3(1) and 3(3): Effects vs agreement

Section 3(1) prohibits agreements that cause or are likely to cause an appreciable adverse effect on competition.⁵⁷ An effects based reading suggests that once AAEC is demonstrated, subjective intent becomes secondary, and continued deployment of an AI agent despite foreseeable anti competitive effects can itself be treated as a form of concerted practice.⁵⁸ Indian authorities and practitioners increasingly argue that firms cannot claim ignorance where they knowingly deploy pricing or procurement agents in concentrated, transparent markets and ignore warning signs of coordination.⁵⁹

Section 3(3) creates presumptions for horizontal practices such as price fixing, bid rigging and output limitation.⁶⁰ The challenge in AI cases is linking the “agreement” element to agent behaviour absent human communication.⁶¹ Where a common vendor or platform facilitates alignment, the hub and spoke theory can satisfy the agreement requirement through the intermediary.⁶² Where agents act independently, enforcers may need to rely on structural predisposition, design choices and governance failures to infer an understanding, or advocate de lege ferenda reforms that introduce a targeted presumption for algorithmic pricing systems that produce sustained coordination.⁶³

⁴⁸ Bar & Bench, supra note 2; see also Noah News, supra note 5.

⁴⁹ Trmlabs, supra note 13; see also Scholar Club, supra note 14.

⁵⁰ Competition Act, 2002, § 2(b) (India); see also LiveLaw, Jurisprudential Dilemma of Algorithmic Cartels (Apr. 17, 2026), <https://www.livelaw.in/articles/jurisprudential-dilemma-algorithmic-cartels-530685>.

⁵¹ K SandK, Algorithmic Collusion and Section 3(3) Competition Act (Mar. 2, 2026), <https://ksandk.com/competition/algorithmic-collusion-competition-act/>; see also Bar & Bench, Beyond the Agreement Paradigm: Regulating Algorithmic Collusion under the Competition Act, 2002 (June 30, 2026), <https://www.barandbench.com/columns/beyond-the-agreement-paradigm-regulating-algorithmic-collusion-under-the-competition-act-2002>.

⁵² LiveLaw, supra note 1; see also CBCL NLIU, Addressing Algorithmic Collusion in Indian Competition Law (Dec. 16, 2025), <https://cbcl.nliu.ac.in/competition-law/addressing-algorithmic-collusion-in-indian-competition-law/>.

⁵³ K SandK, supra note 2; see also IRCCL, Algorithmic Collusion and the Limits of Agreement under Indian Competition Law (Feb. 20, 2026), <https://www.irccl.in/post/algorithmic-collusion-and-the-limits-of-agreement-under-indian-competition-law>.

⁵⁴ LiveLaw, Coded Collusion: Algorithmic Pricing in Indian Aviation and Structural Failure of Competition Law (June 9, 2026), <https://www.livelaw.in/articles/algorithmic-pricing-indian-aviation-structural-failure-competition-law-537241>; see also IRCCL, supra note 4.

⁵⁵ Bar & Bench, supra note 2; see also Noah News, India Considers New Legal Framework to Address Algorithmic Collusion Risks (June 30, 2026), <https://noah-news.com/india-considers-new-legal-framework-to-address-algorithmic-collusion-risks/>.

⁵⁶ Competition Act, 2002, § 2(b), § 3(1) (India); see also LiveLaw, supra note 1.

⁵⁷ Competition Act, 2002, § 3(1) (India); see also K SandK, supra note 2.

⁵⁸ K SandK, supra note 2; see also Bar & Bench, supra note 2.

⁵⁹ K SandK, supra note 2; see also CBCL NLIU, supra note 3.

⁶⁰ Competition Act, 2002, § 3(3) (India); see also K SandK, supra note 2.

⁶¹ LiveLaw, supra note 5; see also IRCCL, supra note 4.

⁶² K SandK, supra note 2; see also Reuters, Collusion by Code? Understanding Algorithmic Pricing and Antitrust Enforcement (Mar. 20, 2026), <https://www.reuters.com/legal/legalindustry/collusion-by-code-understanding-algorithmic-pricing-and-antitrust-enforcement--pracin-2026-03-20/>.

⁶³ Bar & Bench, supra note 2; see also Noah News, supra note 6.

4.3 Section 4 (abuse of dominance) and AI agents

Section 4 addresses abuse of dominant position without requiring an agreement.⁶⁴ This makes it a vital tool for AI mediated conduct by dominant firms. A dominant enterprise that deploys self learning pricing agents to engage in predatory pricing, discriminatory tariffs, self preferencing in multi sided platforms or exclusionary contracting may face abuse claims even if no collusion with rivals is provable.⁶⁵ The focus shifts to whether the agent's conduct leverages dominance to distort competition, raise rivals' costs or exploit customers.⁶⁶ Algorithmic opacity does not shield the firm, because Section 4 liability turns on effects and the causal link between dominance and anti competitive conduct, not on consensus among competitors.⁶⁷

4.4 Leniency, settlements, and compliance incentives

The leniency programme under the Competition Act can be adapted to AI cases. Applicants should be required to disclose algorithmic design parameters, data inputs, governance logs and internal risk assessments to qualify for reduced penalties.⁶⁸ This ensures that leniency serves not only to uncover human cartels but also to illuminate how AI agents produced coordinated outcomes.⁶⁹

The 2023 amendments introduced commitments and settlements, allowing parties to offer structural or behavioural remedies to address competition concerns.⁷⁰ In AI cases, the CCI can accept commitments that mandate algorithmic audits, data segregation from competitors, human oversight thresholds for material pricing decisions, and periodic reporting on model performance and market effects.⁷¹ These tools create compliance incentives for firms to invest in AI governance, monitor for unintended coordination and cooperate with authorities, thereby reducing the enforcement burden while preserving deterrence.⁷²

V. Comparative and Global Enforcement Trends

5.1 US: Algorithmic collusion as "old crime, new code"

United States enforcers frame algorithmic collusion as "old crime, new code". The Department of Justice and Federal Trade Commission treat shared pricing tools and common algorithms as potential concerted action, and maintain that criminal exposure remains where a horizontal agreement among competitors is provable.⁷³ The RealPage settlement illustrates this approach. The government alleged that a common pricing software facilitated coordination among landlords, and the settlement imposed liability on both the vendor and users for facilitating and participating in price alignment through algorithmic means.⁷⁴ The lesson is clear: firms cannot claim that the algorithm acted alone, and vendors can be drawn into liability where their product design and data flows enable coordination.⁷⁵

5.2 EU/UK: Priority enforcement on algorithmic pricing

The European Commission and the UK Competition and Markets Authority have identified algorithmic pricing, including agentic AI, as an enforcement priority.⁷⁶ Hub and spoke theories and vendor liability are live doctrines in both jurisdictions.⁷⁷ The Eturas case in the EU established that firms can be liable for algorithm facilitated collusion even with limited awareness, where they continue to use a platform that transmits pricing signals and they fail to

⁶⁴ Competition Act, 2002, § 4 (India); see also K SandK, Indian Competition Law — Complete Guide (Feb. 24, 2026), <https://ksandk.com/competition-review/guides/indian-competition-law/>.

⁶⁵ JD Supra, Algorithmic Pricing and AI Powered Evidence Avoidance (Mar. 27, 2026), <https://www.jdsupra.com/legalnews/algorithmic-pricing-and-ai-powered-1056402/>; see also K SandK, supra note 15.

⁶⁶ JD Supra, supra note 16.

⁶⁷ Competition Act, 2002, § 4 (India); see also K SandK, supra note 15.

⁶⁸ CBCL NLIU, supra note 3; see also K SandK, supra note 15.

⁶⁹ CBCL NLIU, supra note 3.

⁷⁰ K SandK, supra note 15.

⁷¹ Id.; see also Bar & Bench, supra note 2.

⁷² K SandK, supra note 15; see also CBCL NLIU, supra note 3.

⁷³ Reuters, Collusion by Code? Understanding Algorithmic Pricing and Antitrust Enforcement (Mar. 20, 2026), <https://www.reuters.com/legal/legalindustry/collusion-by-code-understanding-algorithmic-pricing-and-antitrust-enforcement--pracin-2026-03-20/>; see also DLA Piper, Old Crime, New Code: DOJ Puts Algorithmic Collusion in Focus (June 11, 2026), <https://www.dlapiper.com/en-us/insights/publications/2026/06/doj-antitrust-division-puts-focus-on-algorithmic-collusion>.

⁷⁴ Reuters, supra note 1; see also Skadden, Algorithmic Pricing Decisions Have Favored Defendants, but the Trend May Be Shifting (Jan. 13, 2026), <https://www.skadden.com/insights/publications/2026/2026-insights/litigation-controversy/algorithmic-pricing-decisions>.

⁷⁵ Reuters, supra note 1.

⁷⁶ Morgan Lewis, Algorithmic Pricing Emerges as Enforcement Priority for EU and UK Antitrust Regulators (Oct. 14, 2025), <https://www.morganlewis.com/pubs/2025/10/algorithmic-pricing-emerges-as-enforcement-priority-for-eu-and-uk-antitrust-regulators>.

⁷⁷ Id.; see also Akin Gump, CMA Highlights Real World Risks of Algorithmic Pricing (Mar. 16, 2026), <https://www.akingump.com/en/insights/alerts/when-bots-set-prices-cma-highlights-real-world-risks-of-algorithmic-pricing>.

distance themselves from the coordinated outcome.⁷⁸ The CMA has similarly warned that the use of AI driven pricing tools increases antitrust compliance risk, and that enforcers will scrutinise deployment choices, data sharing and oversight mechanisms.⁷⁹ These cases signal that subjective intent is not decisive; continued use of a system that foreseeably produces alignment can itself attract liability.⁸⁰

5.3 Brazil and others: Explicit moves on AI pricing

Brazil's Administrative Council for Economic Defense has pursued investigations into AI and machine learning pricing in sectors such as aviation and fuel retail.⁸¹ In one notable development, CADE entered into a termination commitment with a pricing software developer, signalling supplier side accountability where the tool facilitates coordination among competitors.⁸² Beyond enforcement, legislative proposals in other jurisdictions offer comparative models for reform. California's Assembly Bill 325, for example, seeks to ban "common pricing algorithms" that facilitate alignment among rivals, creating a statutory presumption against certain shared algorithmic practices.⁸³ While India need not copy this model, it illustrates how legislatures can target high risk algorithmic conduct directly rather than relying solely on general agreement language.⁸⁴

5.4 Takeaways for India

The global trajectory is consistent: there is no "tech shield" for anti competitive outcomes.⁸⁵ Enforcement focuses on deployment choices, data flows, vendor relationships and oversight failures, not on whether a human manually set each price.⁸⁶ For India, this reinforces the view that the broad "agreement" language in Sections 2(b) and 3 can cover many AI mediated scenarios, especially in hub and spoke or common platform cases.⁸⁷ However, purely autonomous convergence may still strain the agreement paradigm.⁸⁸ Targeted presumptions, disclosure powers for design parameters and data inputs, and mandatory algorithmic audits for high risk pricing systems would align Indian law with emerging global best practice and close the attribution gap without over deterring innovation.⁸⁹

VI. A Proposed Attribution Framework for AI-Agent Conduct

6.1 Guiding principle: Autonomy redistributes, does not eliminate, accountability

The starting point is that AI agents lack legal personhood and cannot be sanctioned.⁹⁰ Responsibility must therefore rest with the humans and entities that design, deploy, authorise or benefit from the system.⁹¹ Autonomy redistributes accountability across this chain but does not eliminate it.⁹² The deploying enterprise should bear primary liability on the theory that it chooses to use the agent for commercial decisions and reaps the benefits, while secondary allocation to developers, vendors and platform providers should turn on control, fault and causal contribution.⁹³

⁷⁸ Akin Gump, *supra* note 5; see also Morgan Lewis, *supra* note 4.

⁷⁹ Akin Gump, *supra* note 5.

⁸⁰ *Id.*; see also Morgan Lewis, *supra* note 4.

⁸¹ Wolters Kluwer, When AI Prices, Who Is Liable? A Brazilian Perspective (June 9, 2026), <https://legalblogs.wolterskluwer.com/competition-blog/when-ai-prices-who-is-liable-a-brazilian-perspective/>.

⁸² *Id.*

⁸³ DLA Piper, Antitrust Meets AI: Plaintiffs, Enforcers, and Legislatures Take Aim at Alleged AI Driven Collusion (Nov. 4, 2025), <https://www.dlapiper.com/en-us/insights/publications/2025/11/antitrust-and-ai-plaintiffs-enforcers-and-legislatures-take-aim-at-alleged-ai-driven-collusion>.

⁸⁴ *Id.*; see also Bar & Bench, Beyond the Agreement Paradigm: Regulating Algorithmic Collusion under the Competition Act, 2002 (June 30, 2026), <https://www.barandbench.com/columns/beyond-the-agreement-paradigm-regulating-algorithmic-collusion-under-the-competition-act-2002>.

⁸⁵ HLC, Update on Algorithmic Pricing in Competition Law (Oct. 14, 2025), <https://www.hlc.com/en/publications/update-on-algorithmic-pricing-in-competition-law-what-you-need-to-know>.

⁸⁶ *Id.*; see also Reuters, *supra* note 1.

⁸⁷ Competition Act, 2002, § 2(b), § 3(1) (India); see also K SandK, Algorithmic Collusion and Section 3(3) Competition Act (Mar. 2, 2026), <https://ksandk.com/competition/algorithmic-collusion-competition-act/>.

⁸⁸ LiveLaw, Coded Collusion: Algorithmic Pricing in Indian Aviation and Structural Failure of Competition Law (June 9, 2026), <https://www.livelaw.in/articles/algorithmic-pricing-indian-aviation-structural-failure-competition-law-537241>.

⁸⁹ Bar & Bench, *supra* note 12; see also Noah News, India Considers New Legal Framework to Address Algorithmic Collusion Risks (June 30, 2026), <https://noah-news.com/india-considers-new-legal-framework-to-address-algorithmic-collusion-risks/>.

⁹⁰ Trmlabs, Autonomous AI Agents and Financial Crime: Risk, Responsibility and Accountability (Feb. 26, 2026), <https://www.trmlabs.com/resources/blog/autonomous-ai-agents-and-financial-crime-risk-responsibility-and-accountability>.

⁹¹ *Id.*; see also IMDA, Legal Responsibility for AI Agents (May 21, 2026), <https://www.imda.gov.sg/-/media/imda/files/about/emerging-tech-and-research/artificial-intelligence/agents-legal-responsibility.pdf>.

⁹² Trmlabs, *supra* note 1.

⁹³ IMDA, *supra* note 2; see also Trmlabs, *supra* note 1.

6.2 Control–Authorization–Duty–Causation–Rule (CADCR) test

To operationalise this principle, adjudicators can apply a Control, Authorisation, Duty, Causation and Rule test adapted from recent scholarship on autonomous agents.⁹⁴

Control asks who had technical and operational control over the agent's objective function, training data, data inputs and deployment environment.⁹⁵ A firm that sets the reward function for a pricing agent, selects the data feeds and controls deployment parameters exercises substantial control and should be treated as the principal actor.⁹⁶

Authorisation examines the scope of authority granted to the agent. What pricing bands, negotiation parameters and counterparty classes were pre approved? Was there a human in the loop for material decisions, and could humans override the agent in real time?⁹⁷ Where an agent operates within clear mandates and the firm ratifies its outcomes, attribution to the firm is straightforward.⁹⁸

Duty focuses on compliance obligations. Did the firm conduct algorithmic audits, monitor for coordination patterns, segregate non public competitor data and perform vendor due diligence?⁹⁹ Breach of these duties indicates fault and supports liability even where intent is opaque.¹⁰⁰

Causation requires linking the anti competitive outcome to design or deployment choices rather than pure market noise.¹⁰¹ Audit trails, version control, and counterfactual simulations can help establish that the agent's conduct, as deployed, was a substantial cause of the harmful effect.¹⁰²

Rule selection then determines the liability rule and allocation. Depending on the answers above, adjudicators may apply strict liability to the deploying firm for high risk use cases, negligence based liability where oversight failed, or vicarious liability where the agent acted within apparent authority.¹⁰³ Developers and vendors may face joint or several liability where they knowingly design for alignment or facilitate hub and spoke coordination.¹⁰⁴

6.3 Enterprise-risk model for the deploying firm

Under an enterprise risk model, primary liability rests with the firm that deploys the agent for pricing, negotiation or procurement.¹⁰⁵ The firm is best placed to assess market structure, foresee coordination risks and implement governance.¹⁰⁶ Defences and mitigation should include robust AI governance frameworks, pre deployment testing for collusion risk, continuous monitoring of market outcomes, and prompt remediation when red flags appear.¹⁰⁷ Where such measures are documented and effective, penalties can be reduced even if AAEC occurs.¹⁰⁸

6.4 Vendor and platform liability (hub-and-spoke)

Where a common algorithm or platform enables coordination, vendors and intermediaries can be liable if they knowingly facilitate or design for alignment.¹⁰⁹ Global cases show that pricing software providers can face enforcement where their product ingests competitors' data and produces aligned

⁹⁴ Scholar Club, Attributing Legal Liability for Autonomous AI Agents in Crypto Asset Markets, J. L. & Soc. Sci. (Aug. 11, 2026), <https://scholarclub.org/index.php/jllsa/article/view/249>.

⁹⁵ Trmlabs, supra note 1.

⁹⁶ Id.

⁹⁷ IMDA, supra note 2.

⁹⁸ Id.; see also Scholar Club, supra note 5.

⁹⁹ Reuters, Collusion by Code? Understanding Algorithmic Pricing and Antitrust Enforcement (Mar. 20, 2026), <https://www.reuters.com/legal/legalindustry/collusion-by-code-understanding-algorithmic-pricing-and-antitrust-enforcement--pracin-2026-03-20/>; see also HLC, Update on Algorithmic Pricing in Competition Law (Oct. 14, 2025), <https://www.hlc.com/en/publications/update-on-algorithmic-pricing-in-competition-law-what-you-need-to-know>.

¹⁰⁰ Reuters, supra note 10.

¹⁰¹ CBCL NLIU, Addressing Algorithmic Collusion in Indian Competition Law (Dec. 16, 2025), <https://cbcl.nliu.ac.in/competition-law/addressing-algorithmic-collusion-in-indian-competition-law/>.

¹⁰² Id.

¹⁰³ Scholar Club, supra note 5; see also Digital L. J., Artificial Intelligence and Liability: Exploring Legal Challenges and Responsibility in AI Decision Making and Autonomous Systems (June 5, 2026), <https://www.digitallawjournal.org/jour/article/view/320>.

¹⁰⁴ Scholar Club, supra note 5.

¹⁰⁵ Trmlabs, supra note 1.

¹⁰⁶ Id.

¹⁰⁷ Reuters, supra note 10; see also CBCL NLIU, supra note 12.

¹⁰⁸ Reuters, supra note 10.

¹⁰⁹ Reuters, supra note 10; see also Akin Gump, CMA Highlights Real World Risks of Algorithmic Pricing (Mar. 16, 2026), <https://www.akingump.com/en/insights/alerts/when-bots-set-prices-cma-highlights-real-world-risks-of-algorithmic-pricing>.

outcomes.¹¹⁰ In India, such providers can be treated as “persons” under Section 3 where they orchestrate or enable concerted outcomes, reviving hub and spoke theories under Sections 2(b) and 3(1).¹¹¹

6.5 Statutory reform options (*de lege ferenda*)

De lege ferenda, India could introduce a targeted provision, such as Section 3A, prohibiting the deployment of algorithmic pricing systems that cause or are likely to cause AAEC, with a rebuttable presumption where sustained coordinated outcomes occur.¹¹² This would shift the burden to firms to demonstrate that coordination was not foreseeable or that governance measures were adequate.¹¹³ Complementary powers should include disclosure of design parameters, data inputs and objective functions, and mandatory algorithmic audits for high risk use cases.¹¹⁴

VII. Compliance Architecture for Firms

7.1 Governance and accountability

Firms should appoint a senior AI compliance owner responsible for antitrust risk in commercial AI systems.¹¹⁵ A central register should list all AI agents used in pricing, negotiation and procurement, along with their objectives, data sources and deployment environments.¹¹⁶ Governance policies must define authority limits for each agent, set escalation thresholds for material decisions and mandate human in the loop checkpoints where market impact is significant.¹¹⁷ Clear accountability lines ensure that someone within the firm can explain why an agent was deployed, what safeguards were in place and how red flags were handled.¹¹⁸

7.2 Algorithmic self-audits and testing

Firms should conduct periodic algorithmic self audits to detect unintended coordination patterns.¹¹⁹ These audits should document design choices, training data, objective functions and observed market outcomes, and compare them against counterfactual scenarios.¹²⁰ Red team exercises can simulate collusion risk, for example by testing how the agent behaves when rivals use a common vendor, share data feeds or operate in highly transparent markets.¹²¹ Where audits reveal sustained parallelism or sensitivity to rivals’ moves, firms should adjust parameters, introduce noise or impose stricter human oversight before continuing deployment.¹²²

7.3 Data and vendor management

Data governance is critical. Firms must segregate non public competitor data and avoid ingesting rivals’ confidential information into pricing or procurement models.¹²³ Where common pricing engines or platforms are used, legal vetting should assess hub and spoke risks and document the business justification.¹²⁴ Vendor contracts should include audit rights, compliance warranties and incident reporting obligations, so that the firm can verify how

¹¹⁰ Reuters, *supra* note 10.

¹¹¹ LiveLaw, Jurisprudential Dilemma of Algorithmic Cartels (Apr. 17, 2026), <https://www.livelaw.in/articles/jurisprudential-dilemma-algorithmic-cartels-530685>; see also Competition Act, 2002, § 2(b), § 3(1) (India).

¹¹² Bar & Bench, Beyond the Agreement Paradigm: Regulating Algorithmic Collusion under the Competition Act, 2002 (June 30, 2026), <https://www.barandbench.com/columns/beyond-the-agreement-paradigm-regulating-algorithmic-collusion-under-the-competition-act-2002>; see also Noah News, India Considers New Legal Framework to Address Algorithmic Collusion Risks (June 30, 2026), <https://noah-news.com/india-considers-new-legal-framework-to-address-algorithmic-collusion-risks/>.

¹¹³ Bar & Bench, *supra* note 23.

¹¹⁴ *Id.*; see also Noah News, *supra* note 23.

¹¹⁵ Reuters, Collusion by Code? Understanding Algorithmic Pricing and Antitrust Enforcement (Mar. 20, 2026), <https://www.reuters.com/legal/legalindustry/collusion-by-code-understanding-algorithmic-pricing-and-antitrust-enforcement--pracin-2026-03-20/>.

¹¹⁶ *Id.*; see also CBCL NLIU, Addressing Algorithmic Collusion in Indian Competition Law (Dec. 16, 2025), <https://cbcl.nliu.ac.in/competition-law/addressing-algorithmic-collusion-in-indian-competition-law/>.

¹¹⁷ IMDA, Legal Responsibility for AI Agents (May 21, 2026), <https://www.imda.gov.sg/-/media/imda/files/about/emerging-tech-and-research/artificial-intelligence/agents-legal-responsibility.pdf>.

¹¹⁸ Reuters, *supra* note 1.

¹¹⁹ CBCL NLIU, *supra* note 2.

¹²⁰ *Id.*; see also Bar & Bench, Beyond the Agreement Paradigm: Regulating Algorithmic Collusion under the Competition Act, 2002 (June 30, 2026), <https://www.barandbench.com/columns/beyond-the-agreement-paradigm-regulating-algorithmic-collusion-under-the-competition-act-2002>.

¹²¹ Reuters, *supra* note 1.

¹²² CBCL NLIU, *supra* note 2.

¹²³ Reuters, *supra* note 1; see also HLC, Update on Algorithmic Pricing in Competition Law (Oct. 14, 2025), <https://www.hlc.com/en/publications/update-on-algorithmic-pricing-in-competition-law-what-you-need-to-know>.

¹²⁴ Reuters, *supra* note 1.

the tool works, what data it accesses and whether it facilitates alignment with competitors.¹²⁵ Regular vendor due diligence should evaluate whether the provider's design choices increase coordination risk.¹²⁶

7.4 Evidence preservation and cooperation

Finally, firms should preserve evidence to support leniency or settlement applications if concerns arise.¹²⁷ This includes maintaining version controlled logs of model changes, data inputs, governance approvals and market monitoring reports.¹²⁸ Systems should be designed with sufficient explainability to allow the firm and authorities to reconstruct how a particular pricing or negotiation outcome occurred, and to allocate fault between design, deployment and market factors.¹²⁹ Cooperation with the Competition Commission of India, including early disclosure of algorithmic risks and remedial steps, can mitigate penalties and demonstrate good faith compliance.¹³⁰

VIII. Application to Hypotheticals

8.1 Hypothesis A: Two airlines' self-learning fare agents converge

Two competing airlines independently deploy self learning fare agents that observe public data such as demand, load factors and rivals' published fares.¹³¹ Over several months, their fares converge on key routes despite no shared platform or common vendor.¹³² Under current law, the "agreement" case is weak because there is no communication, common design or hub facilitating coordination.¹³³ Liability would depend on showing that the airlines knowingly adopted similar systems in a concentrated, transparent market and failed to mitigate foreseeable coordination risks.¹³⁴ This scenario supports the case for a Section 3A style presumption where sustained coordinated outcomes trigger a rebuttable burden on firms to demonstrate adequate governance and lack of design level collusion.¹³⁵

8.2 Hypothesis B: E-commerce sellers use a common pricing-agent platform

Several e-commerce sellers subscribe to a common pricing agent platform that ingests non public data on competitors' inventory and promotions and automatically adjusts prices.¹³⁶ Prices across sellers align closely over time.¹³⁷ This is a classic hub and spoke scenario. The platform acts as the hub, and the sellers as spokes who knowingly adopt the system.¹³⁸ "Action in concert" under Section 2(b) is plausible because the sellers consciously participate in a shared mechanism that produces alignment.¹³⁹ Both sellers and the vendor may face joint liability, and the Competition Commission of India can seek disclosures on design and data flows and impose commitments such as data segregation, audit rights and human oversight thresholds.¹⁴⁰

¹²⁵ Morgan Lewis, Algorithmic Pricing Emerges as Enforcement Priority for EU and UK Antitrust Regulators (Oct. 14, 2025), <https://www.morganlewis.com/pubs/2025/10/algorithmic-pricing-emerges-as-enforcement-priority-for-eu-and-uk-antitrust-regulators>.

¹²⁶ Id.

¹²⁷ CBCL NLIU, supra note 2; see also K SandK, Indian Competition Law — Complete Guide (Feb. 24, 2026), <https://ksandk.com/competition-review/guides/indian-competition-law/>.

¹²⁸ CBCL NLIU, supra note 2.

¹²⁹ Id.; see also Scholar Club, Attributing Legal Liability for Autonomous AI Agents in Crypto Asset Markets, J. L. & Soc. Sci. (Aug. 11, 2026), <https://scholarclub.org/index.php/jllsa/article/view/249>.

¹³⁰ K SandK, supra note 13; see also Bar & Bench, supra note 6.

¹³¹ LiveLaw, Coded Collusion: Algorithmic Pricing in Indian Aviation and Structural Failure of Competition Law (June 9, 2026), <https://www.livelaw.in/articles/algorithmic-pricing-indian-aviation-structural-failure-competition-law-537241>.

¹³² Id.; see also IRCCL, Algorithmic Collusion and the Limits of Agreement under Indian Competition Law (Feb. 20, 2026), <https://www.irccl.in/post/algorithmic-collusion-and-the-limits-of-agreement-under-indian-competition-law>.

¹³³ LiveLaw, supra note 1; see also Bar & Bench, Beyond the Agreement Paradigm: Regulating Algorithmic Collusion under the Competition Act, 2002 (June 30, 2026), <https://www.barandbench.com/columns/beyond-the-agreement-paradigm-regulating-algorithmic-collusion-under-the-competition-act-2002>.

¹³⁴ LiveLaw, supra note 1; see also Noah News, India Considers New Legal Framework to Address Algorithmic Collusion Risks (June 30, 2026), <https://noah-news.com/india-considers-new-legal-framework-to-address-algorithmic-collusion-risks/>.

¹³⁵ Bar & Bench, supra note 3; see also Noah News, supra note 4.

¹³⁶ Reuters, Collusion by Code? Understanding Algorithmic Pricing and Antitrust Enforcement (Mar. 20, 2026), <https://www.reuters.com/legal/legalindustry/collusion-by-code-understanding-algorithmic-pricing-and-antitrust-enforcement-pracin-2026-03-20/>; see also Akin Gump, CMA Highlights Real World Risks of Algorithmic Pricing (Mar. 16, 2026), <https://www.akingump.com/en/insights/alerts/when-bots-set-prices-cma-highlights-real-world-risks-of-algorithmic-pricing>.

¹³⁷ Reuters, supra note 6.

¹³⁸ Morgan Lewis, Algorithmic Pricing Emerges as Enforcement Priority for EU and UK Antitrust Regulators (Oct. 14, 2025), <https://www.morganlewis.com/pubs/2025/10/algorithmic-pricing-emerges-as-enforcement-priority-for-eu-and-uk-antitrust-regulators>.

¹³⁹ Id.; see also K SandK, Algorithmic Collusion and Section 3(3) Competition Act (Mar. 2, 2026), <https://ksandk.com/competition/algorithmic-collusion-competition-act/>.

¹⁴⁰ Morgan Lewis, supra note 8; see also K SandK, Indian Competition Law — Complete Guide (Feb. 24, 2026), <https://ksandk.com/competition->

8.3 Hypothesis C: Dominant firm's procurement agent excludes rivals

A dominant firm deploys a procurement agent that dynamically negotiates exclusive supply contracts with key suppliers, raising rivals' costs and limiting their access to inputs.¹⁴¹ No agreement with competitors is involved.¹⁴² This falls squarely under Section 4 abuse of dominance.¹⁴³ The analysis focuses on whether the agent's conduct leverages dominance to distort competition through exclusionary design, such as automatic escalation clauses or loyalty rebates that foreclose rivals.¹⁴⁴ Algorithmic execution does not shield the firm, because Section 4 turns on effects and causal link between dominance and anti competitive conduct, not on consensus among competitors.¹⁴⁵

IX. Counterarguments and Limits

9.1 Over-deterrence and innovation chill

A principal concern is that strict attribution may chill beneficial AI adoption in pricing and procurement.¹⁴⁶ Firms may avoid advanced agents even where they improve efficiency, dynamic discounting and consumer welfare, for fear of being penalised for emergent behaviour they cannot fully predict.¹⁴⁷ The response is to adopt risk based, proportionate duties rather than outcome based strict liability across the board.¹⁴⁸ Safe harbours can be created for audited, low risk designs that meet specified governance standards, such as documented testing, data segregation and human oversight thresholds.¹⁴⁹ Emphasis should lie on whether the firm implemented reasonable compliance measures, not solely on whether coordination occurred.¹⁵⁰

9.2 Epistemic limits and false positives

Another concern is epistemic. In fast moving digital markets, it is difficult to distinguish collusion from competitive parallelism, especially when algorithms react to the same public signals.¹⁵¹ Over enforcement risks false positives that punish normal competition.¹⁵² This risk can be mitigated by requiring sustained patterns of alignment coupled with structural predisposition and design evidence, such as shared data feeds or common objective functions.¹⁵³ Rebuttable presumptions should allow firms to present audit logs, counterfactual simulations and internal risk assessments to show that coordination was not foreseeable or that governance was adequate.¹⁵⁴

9.3 Personhood for AI? (Rejecting electronic legal personality)

Some scholars propose granting AI agents electronic legal personality to simplify attribution.¹⁵⁵ This should be rejected. Personhood would dilute accountability by creating a separate legal entity with no assets or capacity to be sanctioned, while complicating remedies and enforcement.¹⁵⁶ The preferable approach is to attribute conduct to existing legal persons through control and benefit based tests, ensuring that responsibility remains with those who design, deploy and profit from the system.¹⁵⁷

review/guides/indian-competition-law/.

¹⁴¹ JD Supra, Algorithmic Pricing and AI Powered Evidence Avoidance (Mar. 27, 2026), <https://www.jdsupra.com/legalnews/algorithmic-pricing-and-ai-powered-1056402/>.

¹⁴² Id.

¹⁴³ Competition Act, 2002, § 4 (India); see also K SandK, supra note 10.

¹⁴⁴ JD Supra, supra note 11.

¹⁴⁵ Competition Act, 2002, § 4 (India); see also K SandK, supra note 10.

¹⁴⁶ Zenodo, Regulatory Architectures for Autonomous AI Agents: A Comparative Jurisprudential Analysis of UK and EU Frameworks (Feb. 27, 2026), <https://zenodo.org/records/18806260>.

¹⁴⁷ Id.

¹⁴⁸ Bar & Bench, Beyond the Agreement Paradigm: Regulating Algorithmic Collusion under the Competition Act, 2002 (June 30, 2026), <https://www.barandbench.com/columns/beyond-the-agreement-paradigm-regulating-algorithmic-collusion-under-the-competition-act-2002>.

¹⁴⁹ Id.; see also Noah News, India Considers New Legal Framework to Address Algorithmic Collusion Risks (June 30, 2026), <https://noah-news.com/india-considers-new-legal-framework-to-address-algorithmic-collusion-risks/>.

¹⁵⁰ Bar & Bench, supra note 3.

¹⁵¹ LiveLaw, Coded Collusion: Algorithmic Pricing in Indian Aviation and Structural Failure of Competition Law (June 9, 2026), <https://www.livelaw.in/articles/algorithmic-pricing-indian-aviation-structural-failure-competition-law-537241>.

¹⁵² Id.

¹⁵³ Bar & Bench, supra note 3; see also Noah News, supra note 4.

¹⁵⁴ Bar & Bench, supra note 3.

¹⁵⁵ Zenodo, supra note 1.

¹⁵⁶ Id.

¹⁵⁷ Id.; see also Trmlabs, Autonomous AI Agents and Financial Crime: Risk, Responsibility and Accountability (Feb. 26, 2026), <https://www.trmlabs.com/resources/blog/autonomous-ai-agents-and-financial-crime-risk-responsibility-and-accountability>.

X. Conclusion

The rise of AI agents as autonomous economic actors exposes a structural mismatch between competition law's human centred doctrines and the realities of algorithmic markets. As this paper has shown, the core challenge is not whether AI mediated conduct can harm competition, but how to attribute that conduct to legal persons in a manner that preserves deterrence without stifling innovation. Under the Competition Act, 2002, Sections 2(b) and 3 provide sufficient breadth to capture many AI facilitated scenarios, particularly where common platforms, shared data feeds or hub and spoke arrangements enable coordination. Yet purely autonomous convergence by self learning agents strains the "meeting of minds" paradigm and risks an enforcement gap where harmful effects exist but no human consensus is provable.

The proposed solution is an enterprise risk and attribution framework. Primary liability should rest with the deploying firm, which chooses to use the agent for commercial decisions and reaps the benefits. The CADCR test offers adjudicators a structured method to allocate secondary liability across developers, vendors and beneficiaries based on control, authorisation, compliance duties and causal contribution. De lege ferenda, a targeted provision such as Section 3A, coupled with disclosure powers and mandatory algorithmic audits for high risk use cases, would align Indian law with emerging global best practice.

Ultimately, autonomy redistributes but does not eliminate accountability. Indian competition law should evolve from a purely consensus based model to one that ties liability to control, foreseeability and enterprise benefit, ensuring that firms cannot outsource compliance to code while still enabling responsible innovation in commercial AI.