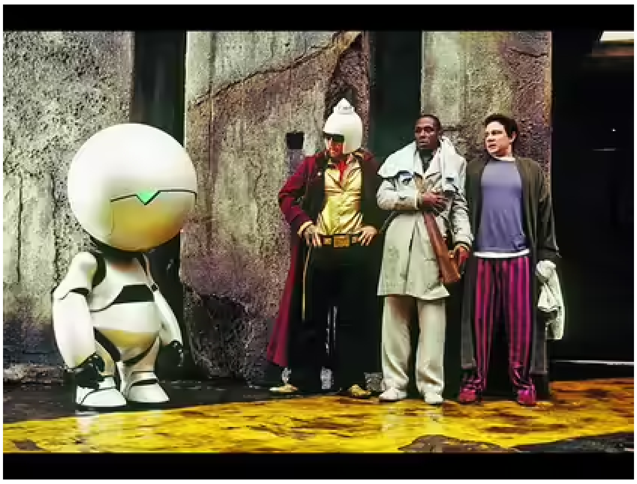
Will machines take the fall? Firms operating in AI-enabled markets need to anticipate, govern and own competition risks

ET economictimes.indiatimes.com/opinion/et-commentary/will-machines-take-the-fall-firms-operating-in-ai-enabled-markets-need-to-anticipate-govern-and-own-competition-risks/printarticle/129809373.cms

Aparna Mehra, Krithika Ramesh, Sarthak Mishra



No humans, the buck stops with you lot

AI is no longer a mere back-office efficiency tool. Across sectors, AI systems are increasingly making decisions that shape market outcomes. As firms deploy algorithms to optimise prices, rank products, personalise offers and manage supply chains, competition authorities worldwide are grappling with a fundamental question: how should competition law respond when market conduct is driven not by human deliberation but by machines or systems?

The regulatory answer is less dramatic than headlines suggest, but potentially more consequential. Rather than rewriting competition law from scratch, regulators appear to be recalibrating how responsibility is assessed - shifting focus from human intent towards attribution, foreseeability and control over AI systems.

Competition regulators have been consistent in recognising that AI can enhance efficiency, lower costs and intensify competition. At the same time, they have identified a recurring set of competition risks associated with algorithmic decision-making. One such risk is algorithmic collusion.

Pricing algorithms that learn from market data and respond to competitors' behaviour can, in some circumstances, converge on price-aligned outcomes without any explicit agreement between firms. This risk is amplified where multiple competitors rely on the same third-party pricing software, creating what authorities describe as 'hub-and-spoke' coordination through shared tools.

Global trends confirm this concern. Competition agencies and authorities in G7 have extensively documented how 'self-learning' algorithms can drift into tacit collusion. In the US, Department of Justice's recent action against RealPage, a provider of property management software, alleges that using shared software to price rents constitutes a modern cartel.

The lesson here is stark: using third-party software does not immunise a company from liability. As US enforcers noted, 'training a machine to break the law is still breaking the law'.

To prove a cartel exists, regulators look for a 'meeting of minds' - a 'smoky room' agreement, or a trail of emails, WhatsApp messages, or any form of evidence where competitors agree to fix prices. But what happens when the collusion is engineered not by humans but by machines?

Autonomous systems can optimise toward profit-maximising outcomes, learn from repeated interactions and adapt behaviour over time, sometimes producing results that resemble collusion without any planning or coordination. Establishing a 'meeting of minds' is far more difficult when decisions are decentralised across algorithms reacting to data rather than conversations and communications between executives.

At the same time, regulators have been clear that the absence of human intent does not immunise firms from liability. As several authorities have put it, training or deploying an algorithm that produces anti-competitive outcomes is still conduct attributable to the firm.

Indian regulators are acutely aware of this gap. Recent regulatory discussions indicate a pivot in how liability is viewed. We are seeing a shift from human intent-based liability ('Did you mean to collude?) to attribution-based accountability ('Did you control the system that colluded?).

This view also featured in discussions at the India AI Impact Summit 2026 last month, where policymakers, industry participants and academics repeatedly returned to the question of who bears responsibility when autonomous systems influence market outcomes. The consensus building across jurisdictions is that if you deploy the AI, you own the outcome. It does not matter if the algorithm is a 'black box', or if it was purchased from a third-party vendor. The deployer is responsible for the governance, risk management and ultimate behaviour of that system.

Competition authorities, in particular, appear to be converging on the view that auditability, transparency and internal oversight are essential for effective enforcement in AI-driven markets. Where algorithms influence prices, rankings or access to consumers, regulators are signalling that firms must be able to explain, not necessarily every line of code, but the logic, data sources and guard rails governing those systems.

Firms are expected to understand mainly:

How their AI systems function.

What data they rely on.

How outputs are generated.

Whether those outputs could foreseeably distort competition.

An effective self-audit must ask the hard questions: does this pricing tool use non-public competitor data? Does the algorithm prioritise our own products over rivals (self-preferencing)? Can we explain why the AI made a specific pricing decision?

For businesses, there are three concrete implications:

Understanding AI systems is no longer just a technical or ethical concern. It's becoming a competition law obligation. Firms cannot rely on 'black box' explanations when algorithms influence market outcomes.

Documentation matters. Clear records of design choices, data sources, monitoring processes and human oversight can be critical in demonstrating that risks were assessed and managed. In fast-moving AI markets, governance may matter as much as outcomes.

Firms should expect enforcement to follow understanding. Competition authorities are still building internal expertise. But their expectations are clear. As regulators become more comfortable interrogating algorithms, the margin for plausible deniability is likely to shrink.

AI doesn't require a wholesale rewrite of competition law. But it's quietly reshaping how responsibility is assigned. For firms operating in AI-enabled markets, the question is no longer whether algorithms can create competition risks. It's whether those risks are being anticipated, governed and owned.