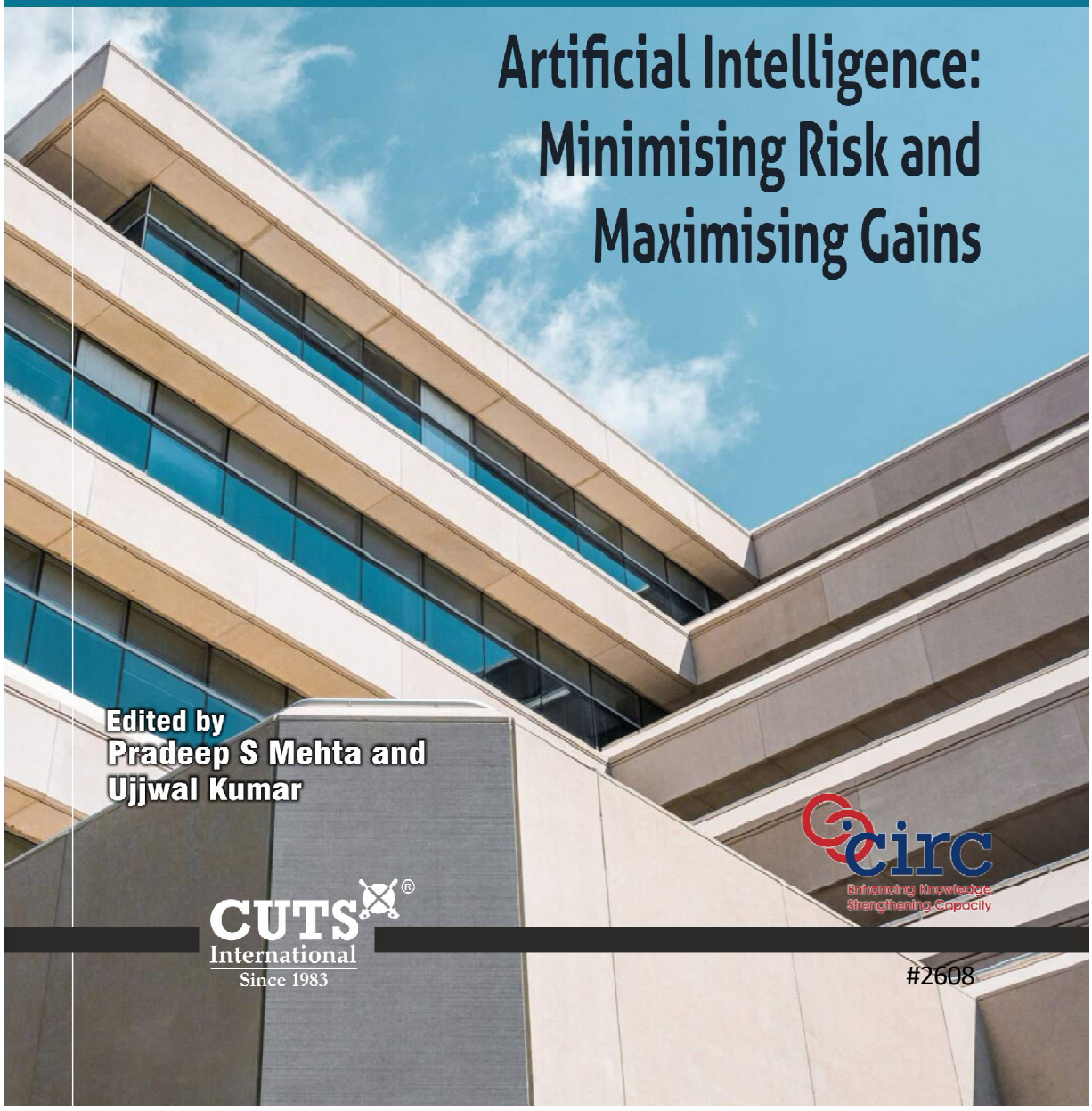
Competition and Regulation in India 2025

Artificial Intelligence: Minimising Risk and Maximising Gains



Edited by
Pradeep S Mehta and
Ujjwal Kumar

CUTS International
Since 1983

CUTS circ
Enhancing Knowledge
Strengthening Capacity

#2608

Competition and Regulation in India, 2025

Artificial Intelligence: Minimising Risks and Maximising Gains

CUTS International
Since 1983

circ
Enhancing Knowledge, Strengthening Capacity

Competition and Regulation in India, 2025

Artificial Intelligence: Minimising Risks and Maximising Gains

Published by:

Consumer Unity & Trust Society
D-217, Bhaskar Marg, Bani Park,
Jaipur 302 016, India
Ph: +91.141.2282821
Fax: +91.141.2282485
Email: cuts1@cuts.org
Website: www.cuts-international.org

CUTS offices also at Kolkata, Chittorgarh and New Delhi (India); Lusaka (Zambia); Nairobi (Kenya); Accra (Ghana); Hanoi (Vietnam); Geneva (Switzerland); and Washington DC (USA)

&

CUTS Institute for Regulation & Competition
Flat No. 5, House No. 658
Lane No. 4, Westend Marg
Saidulajab
New Delhi 110 030, India
Ph: +91.11.46170236
Email: circ@circ.in
Website: www.circ.in

Edited by:
Pradeep S Mehta, Secretory General, CUTS International
Ujjwal Kumar, Associate Director, CUTS International

Citation:
Mehta, Pradeep S and Ujjwal Kumar (Eds.) (2025), Competition and Regulation in India, 2025, CUTS, Jaipur

#2609, Suggested Contribution: ₹395/US$50

Contents

List of Figures

Foreword

It is a privilege to introduce this edition of the India Competition and Regulation Report, devoted to artificial intelligence and its far-reaching implications for India's markets, governance, and society. Artificial intelligence is no longer a niche technology. It is now integral to how goods and services are produced, distributed, discovered, and consumed. AI is changing competitive dynamics through data driven advantages, algorithmic decision making, platform gatekeeping, and new modes of entry and exclusion. The task facing policymakers is therefore twofold, to enable the innovation and economic value that AI can deliver, and at the same time to guard against concentrations of market power and harms to consumers, workers, and democratic discourse.

The Standing Committee on Finance has recently examined the evolving role of the Competition Commission of India in the digital economy. The Committee's report offers insights that are directly relevant to AI policy. The report underlines the need to move from a purely ex post approach to a more forward-looking *ex-ante* posture in digital markets, because practices such as self-preferencing, predatory pricing, and algorithmic steering can entrench dominance quickly. The report also discusses the proposed designation of Systematically Significant Digital Enterprises and calls for careful calibration of thresholds and a rebuttal mechanism to avoid unintentionally capturing fast-growing domestic firms. These practical observations frame many of the regulatory trade-offs discussed in this volume.

Beyond competition law design, the Committee highlighted several institutional and procedural issues that matter deeply for AI governance. There is a pressing need to strengthen institutional capacity, expand technical expertise in areas, such as data science and algorithmic auditing, and ensure predictable funding to enable timely investigations and effective enforcement. The report also recommends implementing a National Competition Policy to foster a coherent competition culture and better coordination between sectoral regulators and the competition authority. For AI policy these suggestions translate into concrete priorities, including cross agency protocols for information sharing, clear standards for non-price harms such as quality and privacy, and mechanisms to protect the ability of small and medium enterprises to access data and compete on fair terms.

This report addresses those priorities, and more. Contributors in this volume examine questions of data governance, intellectual property, sector-specific impacts in health, cybersecurity risks, labour market transitions and skilling, as well as the social risks created by AI systems. The chapters combine empirical evidence, comparative lessons from other jurisdictions, and policy proposals tailored to India's institutional context. Taken together, the report **underscores** that effective AI policy will require an approach that is adaptive, multidisciplinary, and grounded in democratic values. Regulation should be firm enough to prevent market failure and social harm, and flexible enough to allow experimentation, learning, and innovation.

I commend CUTS, CIRC and all the authors for assembling this thoughtful and timely work. I hope this volume stimulates constructive debate among policymakers, regulators, industry, civil society and academia, and helps India chart a path where AI delivers broad-based prosperity, protects fundamental rights, and promotes fair and contestable markets. The recommendations of the Standing Committee on Finance remain an important guide in this endeavour, and I urge stakeholders to engage with both the ideas contained in this report and the Committee's proposals to build a robust, inclusive, and future-ready AI ecosystem.

Bhartruhari Mahtab
Member of Parliament (Lok Sabha)
Chairperson, Standing Committee on Finance

Preface

As India accelerates its adoption of artificial intelligence (AI) across industry, government, and everyday life, policymakers, businesses, regulators, and civil society confront a complex set of trade offs: how to harness AI's productivity and innovation gains while safeguarding competition, consumer welfare, privacy, and democratic discourse. The India Competition and Regulation Report (ICRR) 2025, themed "*Artificial Intelligence: Minimising Risks and Maximising Gains*," brings together legal analysis, sectoral perspectives, empirical reflection, and policy research to map these challenges and offer evidence based responses tailored to India's institutional realities and developmental priorities.

This volume takes a pragmatic and interdisciplinary approach. AI is not merely a technical phenomenon; it is reshaping market structures, strategic conduct, and regulatory boundaries in ways that touch competition law, intellectual property, data governance, sectoral regulation, cybersecurity, and employment. Contributors—from legal practitioners and policy researchers to sector specialists—examine these intersections with an eye to concrete policy levers that preserve contestability, protect consumers, and foster innovation.

The chapters balance conceptual clarity with operational detail: from doctrines addressing tacit collusion in algorithmic markets, to the copyright questions posed by large scale model training, to healthcare specific trade offs where safety and access must be reconciled.

A recurring theme across the Report is the tension between scale and scrutiny. Many AI systems derive value from large scale data aggregation and platform mediated markets that create durable advantages. These dynamics can heighten risks of concentration, foreclosure, and conduct that undermines competitive outcomes. Yet overly prescriptive regulation risks stifling nascent firms and research. ICRR 2025, therefore, seeks to present calibrated insights—recommending interventions that are measurable, proportionate, and sensitive to the innovation lifecycle.

The Report also foregrounds systemic risks that extend beyond traditional market metrics. Cybersecurity threats, misinformation, model hallucinations, bias, and privacy failures can erode trust and produce social harms that feed back into market dysfunction. Effective regulation will require coordination

across agencies—from competition authorities and data protection bodies to sector regulators and law enforcement—and a mix of *ex post* enforcement and *ex ante* standards where appropriate. Strengthening institutional capacity, building technical expertise, and improving access to data for enforcement emerge as recurring recommendations.

Further, empirical input on perceptions and awareness grounds the Report in how Indian consumers understand AI's benefits and risks as well as regulatory approaches. Practical chapters on skilling and workforce transitions address the distributive effects of AI and outline policy tools to promote inclusive outcomes.

CUTS and CIRC have published the ICRR biennially since 2007, consistently highlighting pressing competition and regulatory issues in India. ICRR 2025 does not offer definitive answers; rather, it aims to spur dialogue, inform regulatory thinking, and support evidence based interventions that promote both innovation and a fair, resilient digital economy.

I invite readers to engage critically with the chapters, test their assumptions against India's rapidly evolving markets, and contribute to the collaborative work of making AI work for all.

Bipul Chattopadhyay
Executive Director, CUTS International

Editor's Note

In India, artificial intelligence (AI) is moving from experimentation to widespread deployment across sectors—from healthcare diagnostics and financial services to customer support and content generation. Analysing AI's impact on markets, institutions, and everyday life has therefore become tangible and urgent, especially as policy conversations accelerate. India has taken notable steps: sectoral guidance, public private initiatives on AI skilling, and early efforts to clarify data governance and safety obligations. Yet regulatory frameworks and enforcement capacities continue to lag behind the pace of technological change.

The India Competition and Regulation Report (ICRR) 2025, themed **"**Artificial Intelligence: Minimising Risks and Maximising Gains,**"** aims to inform this policy dialogue with rigorous, multidisciplinary analysis. AI's implications for competition, consumer protection, intellectual property, cybersecurity, and the workforce are crosscutting and complex. Policymakers must balance enabling innovation and scale with preventing market concentration, protecting vulnerable users, and maintaining system resilience.

The ICRR series, a flagship biennial publication of CUTS International and the CUTS Institute for Regulation & Competition (CIRC) since 2007, has served as an invaluable compendium of policy relevant research, shedding light on the state of competition and regulation in India across sectors and contemporary, cross cutting issues.

The present Report, with 10 chapters, offers a broad range of insights on emerging competition and regulatory issues related to AI development and deployment. It addresses concerns such as algorithmic tacit collusion, copyright issues in generative AI training, sectoral regulation in healthcare, AI related cybersecurity threats, and the broader risk spectrum — misinformation, hallucinations, bias, and privacy — that can distort markets and public discourse. The Report closes with a practical treatment of AI's effects on the workforce and skilling strategies, and an epilogue synthesising policy pathways.

Across chapters, several consistent themes emerge: the need for calibrated, evidence based interventions; stronger inter agency coordination; investment in technical capacity for enforcement; and policies that preserve contestability while enabling responsible innovation. Authors advocate a mix of *ex post*

enforcement and targeted *ex ante* safeguards where systemic risk warrants proactive rules.

Bringing this Report to publication required active participation from several domain experts—from shaping chapter outlines to authoring chapters and providing reviews. Their contributions have been invaluable.

We are especially grateful to all the authors: Vidhi Maharshi, Dr. Drishti Parnami, Jameela Sahiba, Shlok Siddhant, Tanya Kukade, Dr. Milind Antani, Sohom Banerjee, Krishaank Jugiani, and Divya Aggarwal.

We acknowledge process related assistance by Krishaank Jugiani and Vidhi Maharshi, editorial assistance by Madhuri Vasnani, and layout and design by Mukesh Tyagi.

We are deeply grateful to Shri Bhartruhari Mahtab, Member of Parliament (Lok Sabha) and Chairperson, Standing Committee on Finance, for writing the Foreword, and to Bipul Chattopadhyay for writing the Preface.

Special appreciation goes to our readers — policymakers, regulators, industry stakeholders, and civil society — for engaging with this work and helping translate its insights into action. We hope ICRR 2025 fosters continued dialogue on building a competitive, inclusive, and resilient digital economy in India.

Jaipur

Pradeep S. Mehta and **Ujjwal Kumar**
CUTS International

Abbreviations

AAEC	Appreciable Adverse Effect on Competition
ABDHM	Ayushman Bharat Digital Health Mission
AI	Artificial Intelligence
AIBOM	Artificial Intelligence Bill of Materials
API	Application Programming Interface
AWS	Amazon Web Services
BIS	Bureau of Indian Standards
BNS	Bharatiya Nyaya Sanhita
BOM	Bill of Materials
CCI	Competition Commission of India
CCPA	Central Consumer Protection Authority
CDSCO	Central Drugs Standard Control Organisation
CEO	Chief Executive Officer
CERT-In	Computer Emergency Response Team
CJEU	Court of Justice of the European Union
CMA	Cement Manufacturers Association
COMPAT	Competition Appellate Tribunal
CPA	Consumer Protection Act
CSR	Corporate Social Responsibility
CUTS	Consumer Unity & Trust Society
DCB	Digital Competition Bill
DMU	Digital Markets Unit
DPDP	Digital Personal Data Protection
EC	European Commission
EdTech	Educational Technology
e-KYC	Electronic Know Your Customer
EU	European Union
FDI	Foreign Direct Investment
FMCGs	Fast Moving Consumer Goods
FTC	Federal Trade Commission
FY	Financial Year

GCC	Global Capability Centre
Gen AI	Generative Artificial Intelligence
GPU	Graphics Processing Unit
HCPs	Healthcare Professionals
HDI	Human Development Index
IBM	International Business Machines Corporation
ICMR	Indian Council of Medical Research
ICN	International Competition Network
ICRR	India Competition and Regulation Report
IIT	Indian Institute of Technology
IoT	Internet of Things
IP	Intellectual Property
ISACs	Information Sharing and Analysis Centres
ISO	International Organisation for Standardisation
IT Act	Information Technology Act, 2000
IT	Information Technology
KYC	Know Your Customer
LLMs	Large Language Models
LPG	Liquefied Petroleum Gas
MDR	Medical Device Rules, 2017
MeitY	Ministry of Electronics and Information Technology
ML	Machine Learning
MoHFW	Ministry of Health and Family Welfare
MTTD	Mean Time to Detect
MTTR	Mean Time to Respond/Mean Time to Recover
NCIIPC	National Critical Information Infrastructure Protection Centre
NCR	National Capital Region
NCRF	National Cyber Security Reference Framework
NHA	National Health Authority
NIST	National Institute of Standards and Technology
NIT	National Institute of Technology
NITI Aayog	National Institution for Transforming India
NMC	National Medical Commission
NSDC	National Skill Development Corporation
OECD	Organisation for Economic Cooperation and Development
OTP	One-Time Password
Q2	Quarter 2

R&D	Research and Development
RBI	Reserve Bank of India
RMPs	Registered Medical Practitioners
SaMD	Software-as-a-Medical-Device
SBOM	Software Bill of Materials
SEBI	Securities and Exchange Board of India
SME	Small and Medium Enterprise
SOCs	Security Operations Centres
SSNDQ	Small but Significant and Non-Transitory Decrease in Quality
SSNIP	Small but Significant and Non-Transitory Increase in Price
TDM	Text and Data Mining
TFEU	Treaty on the Functioning of the European Union
ToI	The Times of India
TPU	Tensor Processing Unit
TRAI	Telecom Regulatory Authority of India
U.S.	United States
UI	User Interface
UK	United Kingdom
UN	United Nations
UNCTAD	United Nations Conference on Trade and Development
USD	United States Dollar
USFDA	US Food and Drug Administration
WEF	World Economic Forum

CHAPTER 1

An Overview

Competition and Regulation in the AI Era

Artificial Intelligence (AI) is widely recognised as a transformative, general-purpose technology reshaping global economies and societies.[1] India, now a top-five AI country,[2] has seen AI seep into various sectors from industry and retail to healthcare and finance.[3] Government initiatives like the IndiaAI Mission have poured investment into computing infrastructure (now 38,000+ GPUs nationwide) and data platforms.[4] As a result, an estimated 87 percent of Indian enterprises use some form of AI.[5]

AI-powered tools are now beginning to improve accuracy, forecasting, and personalisation – for example, better crop recommendations for farmers, smarter diagnostics in medicine, and adaptive learning in education.[6] These gains promise not only efficiency but also inclusion: a recent NITI Aayog report notes that AI can empower India's 490 million informal workers by extending healthcare, education, skills and financial services, thus boosting productivity across the economy.[7]

However, this deep infusion of AI also raises novel competitive and regulatory challenges. AI's potency depends on scarce inputs such as large datasets, powerful cloud infrastructure and advanced algorithms – which currently cluster in the hands of a few tech giants. For instance, the Competition Commission of India's (CCI) market study[8] observed that firms like Alphabet, Amazon, Meta, Microsoft, OpenAI and Nvidia dominate data processing, computing and AI-model creation.

In turn, these incumbents improve their AI through feedback loops: every new user or transaction generates data that refines their models, further widening the gap to rivals. Such network effects and economies of scale mean AI markets can tip irrevocably towards dominant firms.[9] Put simply, whoever has the most data and compute becomes stronger, making it harder for new entrants and smaller firms to compete on a level playing field.

These dynamics have captured the CCI's attention. In September 2025, CCI released Market Study on AI and Competition, a comprehensive review of

how AI is deployed, where market power lies, and what future issues may emerge. The study maps the entire AI value chain (data → algorithms → compute → applications) and highlights that, while AI use in India is still nascent, its potential is enormous.

At the same time, it warns that AI inputs are highly concentrated, creating bottlenecks and entry barriers. For example, firms that control massive data lakes or exclusive compute networks may extract excessive rents or exclude rivals from accessing essential resources. The CCI study thus sets the foundation for future regulation: it catalogues the technology's promise and perils, identifies market power risks, and suggests that India's competition policy prepare accordingly.[10]

At the legislative level, India has so far resisted enacting any AI-specific or ex ante digital competition legislation. While the proposed Digital Competition Bill (DCB) signals an intent to address competition concerns in digital markets *ex ante*, there is currently no dedicated law governing AI as such unlike the European Union, which has adopted the AI Act[11] to impose sector-wide, risk-based obligations on AI systems.

Against this backdrop, India's competition law discourse on AI is entering a formative but cautious phase. The CCI is increasingly signalling readiness to adapt existing doctrines under the Competition Act, 2002 to AI-driven markets. Ongoing debates centre on how traditional concepts such as dominance, abuse, collusion, and foreclosure apply in data-intensive and algorithmically mediated environments, including concerns around self-preferencing by digital platforms, algorithmic price coordination, exclusive access to data or compute, and the competitive effects of strategic partnerships between AI developers and cloud providers.

At the same time, Indian policymakers remain wary of overregulation that could stifle innovation in a still-nascent ecosystem. This has led to a mix of approaches like reliance on market studies, stakeholder consultations, and case-by-case enforcement rather than prescriptive rules. In effect, India is positioning competition law as a flexible, adaptive tool capable of addressing AI-related concentration and exclusion risks while preserving room for technological growth, domestic innovation, and broader public-interest objectives.

An Overview of the 2025 Report

This edition of the ICRR, themed *Artificial Intelligence: Minimising Risks and Maximising Gains,* comprises chapters that examine the interface between AI, regulation, and competition policy in India. As AI systems increasingly shape markets, public services, and everyday decision-making, the report

engages with the dual challenge of harnessing AI's transformative potential while addressing the risks it poses to competition, consumer welfare, and inclusive growth.

The report provides insights on whether existing legal and regulatory frameworks are adequately equipped to respond to AI-driven market dynamics, or whether further interventions are required to prevent exclusionary practices, systemic risks, and regulatory blind spots. Drawing on competition law, sectoral regulation, and comparative international developments, this edition seeks to contribute to a balanced policy discourse one that safeguards innovation and efficiency gains while ensuring accountability, contestability, and equitable access to the benefits of AI in India. The following paragraphs illustrate various chapters in this edition of ICRR.

Chapter 2: Perception and Awareness Reporting

Chapter 2 is a recurring feature of the ICRR that presents survey-based insights into consumer awareness and perceptions of competition regulation in India, with a specific focus in this edition on digital markets and AI–driven services. The chapter is based on a dip stick, yet targeted, survey of 60 respondents to capture nuanced perspectives on regulatory awareness, market fairness, and everyday interactions with AI-enabled platforms.

Chapter 3: Emerging Competition Issues in AI

Chapter 3 explores the broader competition concerns arising from the rapid adoption of AI across markets. It examines how control over key AI inputs such as data, computing infrastructure, and foundational models can entrench market power and raise entry barriers, particularly for start-ups and smaller firms. The chapter discuss all the competition law issues in respect to AI and also analyses challenges for competition authorities in applying traditional concepts of dominance, abuse, and foreclosure to AI-driven markets, while highlighting the need for adaptive enforcement and regulatory coordination to address risks without undermining innovation.

Chapter 4: Artificial Intelligence and Tacit Collusion: An Indian Competition Law Perspective

Chapter 4 focuses specifically on the risks posed by algorithmic decision-making to competitive market outcomes. It analyses how pricing, demand forecasting, and optimisation algorithms can facilitate tacit collusion by enabling firms to monitor rivals, rapidly adjust prices, and converge on coordinated outcomes without explicit communication. The chapter discusses the evidentiary and enforcement difficulties such conduct creates for competition authorities and evaluates whether existing legal standards on agreement and concerted practices are sufficient to capture algorithm-facilitated coordination.

Chapter 5: The Copyright Conundrum of Generative AI Training: An Indian Legal Analysis

Chapter 5 examines the complex and evolving copyright questions raised by the training of generative AI systems, with a particular focus on Indian copyright law. It unpacks how generative artificial intelligence (genAI) models learn from vast corpora of data and interrogates whether acts such as copying, storage, and data ingestion during training amount to copyright infringement.

The chapter analyses key doctrinal touchstones, including the idea–expression dichotomy, transformative use, and the legal relevance of transient or incidental storage, while situating these debates within competing conceptions of copyright protection in the AI era. Moving beyond doctrinal analysis, it evaluates emerging policy responses such as text and data mining exceptions and assesses the limitations of alternative regulatory approaches. Ultimately, the chapter argues for a pragmatic, balanced framework that protects creators' rights without unduly constraining innovation, and charts a forward-looking path for Indian copyright law in response to generative AI.

Chapter 6: Regulation of AI for Healthcare in India

Chapter 6 explores the rapidly evolving landscape of artificial intelligence in healthcare in India, examining its transformative applications, the fragmented yet developing regulatory framework, and the complex legal, ethical, and competition-related challenges that accompany its adoption. It situates India's approach within global regulatory trends, analyses how AI-driven healthcare tools are governed under existing medical device, data protection, consumer protection, intellectual property, and competition laws, and highlights the practical difficulties of regulating adaptive AI systems within traditional legal structures.

The chapter further identifies key risks such as bias, data privacy, accountability, and market concentration, while also considering emerging technologies beyond software-based medical devices. It concludes by underscoring the urgent need for adaptive, risk-based, and coordinated regulation to ensure that AI enhances healthcare outcomes in India while safeguarding patient safety, equity, and public trust.

Chapter 7: Cyber Threats in the Age of AI: Securing the Digital Frontier

This chapter analyses how AI is reshaping cybersecurity for both attackers and defenders, intensifying a data-driven technological arms race. It traces the evolution from largely manual and opportunistic attacks to sophisticated AI-enabled operations, including deepfake-driven social engineering, self-directing malware, and rapid vulnerability discovery. It also examines how defenders respond through AI-supported threat hunting, anomaly detection,

and automated incident response. With a particular focus on India, the chapter evaluates systemic vulnerabilities affecting critical infrastructure, regulatory and governance gaps, skills shortages, and supply-chain dependencies, drawing on both global and domestic case studies.

The chapter advocates for a human-in-the-loop, defence-in-depth strategy supported by a coordinated governance framework such as Software Bill of Materials (SBOM) and Artificial Intelligence Bill of Materials (AIBOM) transparency, risk-based audits of high-impact AI systems, sector-specific reforms, competition policy measures and strengthened public–private threat-intelligence sharing. Finally, the chapter concludes with a comprehensive roadmap that translates these principles into measurable outcomes.

Chapter 8: AI and the Risk Spectrum: Misinformation, Hallucinations, Bias, and Privacy

This chapter examines the complex and evolving societal risks associated with genAI in India, with a particular focus on misinformation, hallucinations, algorithmic bias, and privacy harms arising from AI-generated content and automated decision-making systems. It analyses how these risks are intensified by India's distinctive social and digital context, including linguistic diversity, uneven digital literacy, and socio-economic inequalities.

The chapter explores how genAI systems can amplify misinformation, produce biased or exclusionary outputs, and compromise individual privacy, especially among digitally vulnerable populations. By situating these harms within broader market and institutional dynamics, the chapter highlights how concentration of control over data, compute, and foundational models exacerbates accountability gaps and limits corrective competitive pressures. It evaluates the extent to which India's existing legal and regulatory framework, including the Information Technology Act, sectoral rules, and data protection law try to address these layered risks, identifying gaps in the regulatory framework.

The chapter argues for a balanced, risk-based governance approach that combines technical safeguards, calibrated legal obligations, and competition remedies to mitigate harms while supporting responsible AI innovation in India.

Chapter 9: The AI-Workforce Equation: Skilling for a Transforming Economy

This chapter explores the AI–workforce equation in India by examining how unequal access to AI education and skilling opportunities across Tier 1, Tier 2, and Tier 3 cities, as well as urban–rural divides, is shaping labour market outcomes and economic efficiency. It analyses how urban-centric skilling ecosystems, infrastructure constraints, and limited awareness have

led to the underutilisation of human capital in smaller towns and rural areas, despite India's broader digital transformation goals.

Drawing on a mixed-methods approach, including an original nationwide survey of students and early-career professionals alongside secondary data, the chapter maps regional disparities in awareness, access, infrastructure, and perceived barriers to AI skilling. It concludes by advancing policy and regulatory recommendations focused on inclusive human capital development, such as region-specific skilling mandates, strengthened oversight of private skill providers, public–private partnerships for regional language content, and mandatory transparency in participation and placement outcomes, positioning regional inclusion as essential to India's economic competitiveness in the AI era.

Endnotes

1 https://www.oecd.org/content/dam/oecd/en/publications/reports/2024/05/artificial-intelligence-data-and-competition_9d0ac766/e7e88884-en.pdf

2 https://hai.stanford.edu/assets/files/global_ai_vibrancy_tool_paper_november2024.pdf

3 https://www.pib.gov.in/PressReleasePage.aspx?PRID=2178092&reg=3&lang=2.

4 *Ibid.*

5 https://cio.economictimes.indiatimes.com/news/brand-solution/transforming-hr-in-india-the-imperative-role-of-ai-for-businesses/125532783.

6 https://law.asia/competition-law-expert-discusses-ccis-ai-market-study/.

7 https://niti.gov.in/sites/default/files/2025-09/AI-for-Viksit-Bharat-the-opportunity-for-accelerated-economic-growth.pdf.

8 https://www.cci.gov.in/images/marketstudie/en/market-study-on-artificial-intelligence-and-competition1759752172.pdf.

9 Supra 1.

10 Supra 7.

11 https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=OJ:L_202401689.

CHAPTER 2

Perception and Awareness Reporting

Introduction

The perception and awareness survey on competition, regulation, and emerging digital technologies in India was conducted to understand how consumers perceive regulatory institutions, market conditions, and the growing role of AI in everyday economic interactions. As digital platforms, algorithmic decision-making, and AI-powered services increasingly shape consumer choice and access to markets, it becomes essential to examine whether regulatory awareness and consumer protection mechanisms are keeping pace with technological change.

This chapter presents findings from a dipstick survey of 60 respondents,[1] aimed at providing directional insights on awareness of consumers on the Competition Commission of India (CCI), perceptions of regulatory quality, and lived experiences with AI-driven services, including generative AI tools, recommendation systems, and automated customer support chatbots.

Given the exploratory nature of this study, the survey focused on a smaller, targeted group of respondents, who were graduates and above, mostly employed, to gain in-depth insights into consumer perceptions, providing initial evidence to guide further large-scale studies in this emerging area. The survey further explored consumer concerns about data protection, transparency, fairness, and grievance redressal, as well as public expectations regarding government intervention and regulatory reforms.

The chapter situates consumer experience at the intersection of market power, technology, and regulation by bringing together insights on competition law awareness and AI usage. The findings provide a grounded understanding of how consumers navigate digital markets and what they expect from regulators in ensuring fairness, accountability, and trust.

Awareness of the Competition Commission of India

The survey results indicate a relatively high level of awareness of the Competition Commission of India, with nearly three-fourths of respondents (71.7 percent) reporting that they were aware of the CCI, while 28.3 percent

indicated no awareness. This suggests that while the institution has achieved a degree of public visibility, a significant segment of consumers remains outside its informational reach (Figure 1).

Among respondents who were aware of the CCI, understanding of its role was largely aligned with its statutory mandate. A majority identified the promotion of competition in Indian markets (67.4 percent), combating monopolistic trade practices (65.2 percent), and investigating and adjudicating anti-competitive conduct (63 percent) as key functions of the CCI. These responses indicate that core competition concepts — such as market fairness and prevention of abuse of dominance — resonate with consumers. (Figure 2).

Figure 1: Awareness about CCI (n=60 responses for 60 respondents)

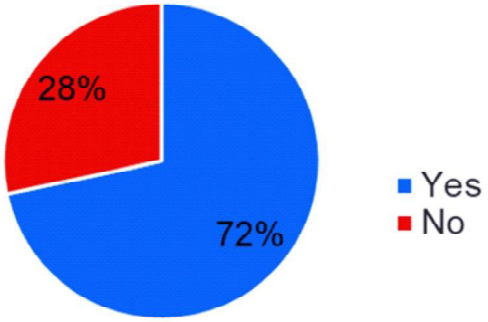
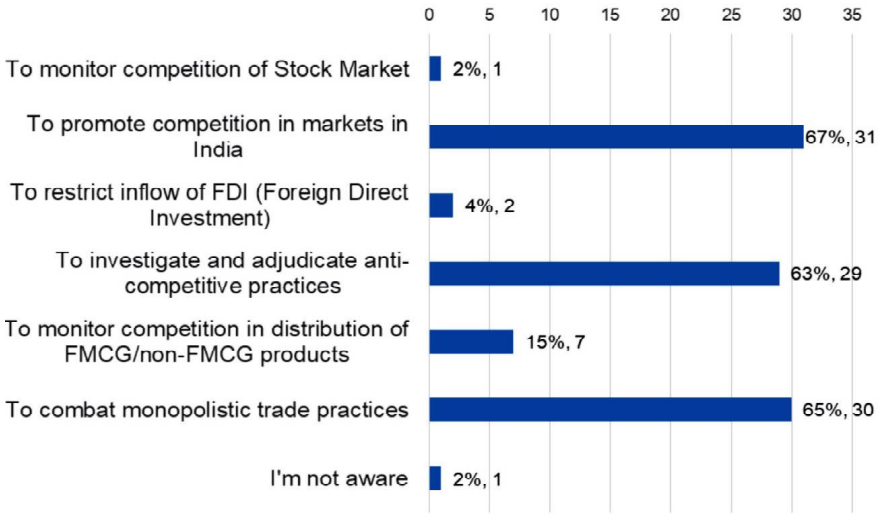


Figure 2: Participants on the Role of CCI (n=101 responses for 46 respondents)

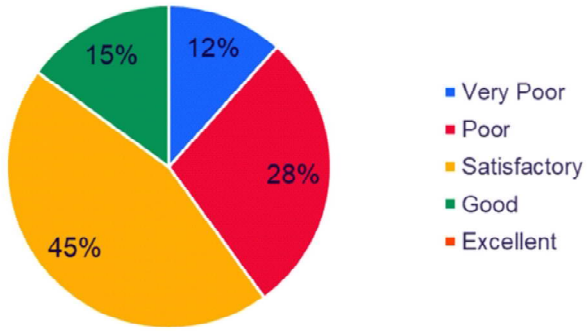


However, the survey also revealed areas of misunderstanding. A small number of respondents attributed responsibilities such as regulating the stock market or restricting foreign direct investment to the CCI, while others associated it with monitoring competition in product distribution networks. Although these responses were limited in number, they highlight the persistence of conceptual overlap in the understanding of economic regulators and underscore the need for clearer institutional communication.

Perceived Quality of Regulation

Perceptions of the overall quality of regulation in India reflect cautious realism rather than strong endorsement. Nearly half of the respondents (45 percent) rated regulatory quality as satisfactory, while 28.3 percent rated it as good. At the same time, a substantial proportion viewed regulation as poor (15 percent) or very poor (11.7 percent). No respondent rated regulatory quality as excellent (Figure 3).

Figure 3: Quality of Regulation (n=60 responses for 60 respondents)



These responses suggest that while regulation is seen as functional, it is not perceived as fully effective or robust. When asked how regulatory quality could be improved, respondents pointed to needing a regulatory system that is professionally competent, autonomous, and insulated from political interference (Figure 4). Weighted scoring[2] shows that respondents prioritise good quality personnel most, followed by reducing political interference and independence of regulatory bodies, highlighting the importance of expertise and minimising undue influence in regulatory effectiveness. Budget allocation is the lowest priority.

Top-rank percentages[3] indicate that reducing political interference is most often seen as the single most critical factor, slightly higher than good quality personnel and independence of institutions. This distinction highlights that while professional expertise and structural autonomy are most valued overall, respondents also consider regulatory independence critically important as a top priority, though budget remains an important supporting factor.

Taken together, these findings indicate that public expectations focus on professional competence, institutional independence, and the capacity to act without undue influence. Regulators are expected to be competent, credible, and insulated from political pressures, with a strong emphasis on human capital and institutional safeguards.

Interaction with AI-Powered Services

The survey highlights widespread engagement with AI-powered services. More than 85 percent of respondents reported having used or interacted with AI tools, with 46.7 percent indicating frequent use and 40 percent reporting occasional use. Only a small number of respondents (11.7 percent) reported no interaction with AI systems, suggesting that AI has become a routine part of the consumer experience (Figure 5).

Figure 4: Response on improvement
(n=60 responses for 60 respondents)

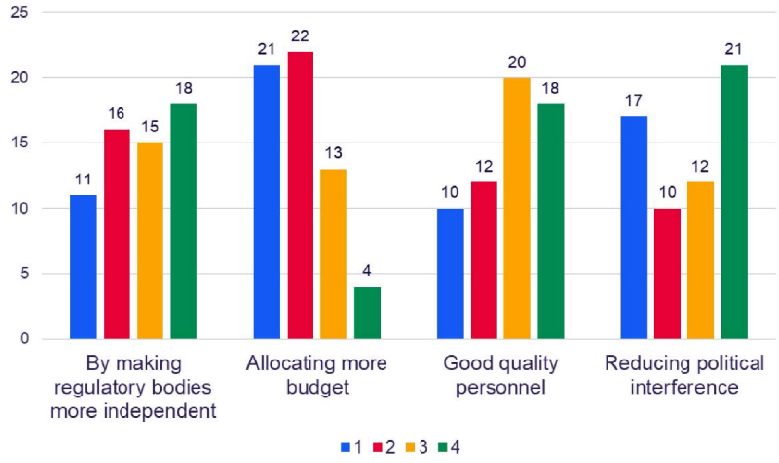
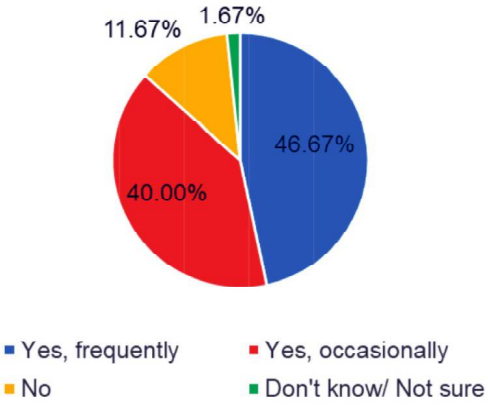
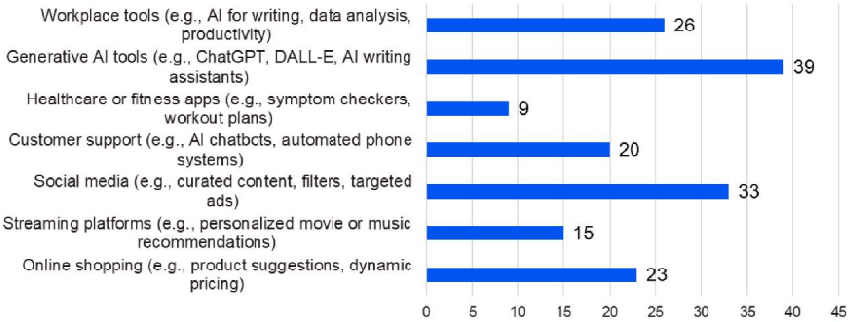


Figure 5: Interaction with AI services
(n=60 responses for 60 respondents)



AI exposure was most commonly reported through generative AI tools such as AI writing assistants, followed by social media platforms where curated content and targeted advertising are prevalent. Workplace productivity tools and online shopping platforms were also major points of interaction, while AI-powered customer support systems featured prominently in service-related contexts. Interaction with AI in healthcare and fitness applications was relatively limited, reflecting either lower adoption or restricted availability (Figure 6).

Figure 6: Interaction with AI (n=165 responses for 58 respondents)



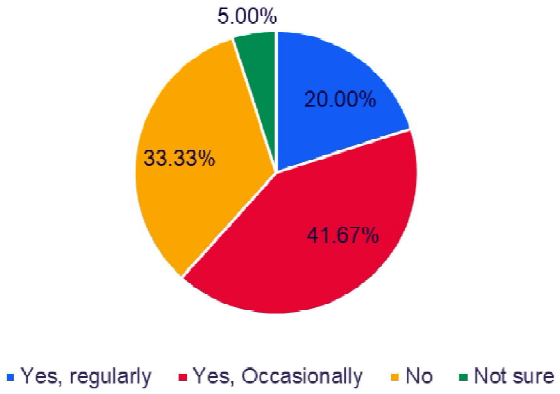
This diversity of AI touch points underscores the breadth of algorithmic influence across consumption, work, and information environments, making questions of accountability and consumer protection increasingly salient.

Use of Multiple AI Platforms

A notable feature of AI usage patterns is the prevalence of multi-platform engagement. Over half of the respondents indicated that they use more than one AI tool either regularly or occasionally for similar purposes. Among these multi-platform users, information comparison or verification emerged as the primary motivation, cited by more than three-fourths of respondents, followed by the search for improved accuracy or enhanced features.

Overall engagement with AI-powered services is relatively high. Around 20 percent respondents reported that they regularly use multiple AI tools or platforms together for similar purposes, while a further 41.7 percent use them occasionally. However, one-third of the respondents that is, 33.3 percent stated that they do not use multiple AI tools or platforms together for similar purposes (Figure 7).

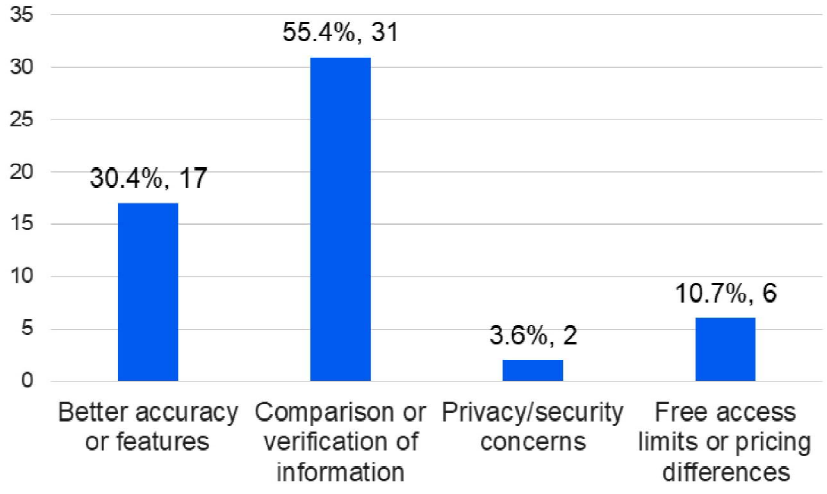
Figure 7: Engagement with AI-powered services (n=60 responses for 60 respondents)



Concerns with AI

Privacy concerns and pricing considerations played only a limited role in using multiple AI tools and platform switching. Just 5 percent of multi-platform users cited privacy or security concerns, and only 15 percent pointed to free access limits or pricing differences. Instead, consumer behaviour appears to be driven primarily by perceived reliability and performance. This pattern suggests relatively low platform loyalty and reflects an underlying trust deficit in individual AI systems, with users relying on cross-verification rather than confidence in a single tool (Figure 8).

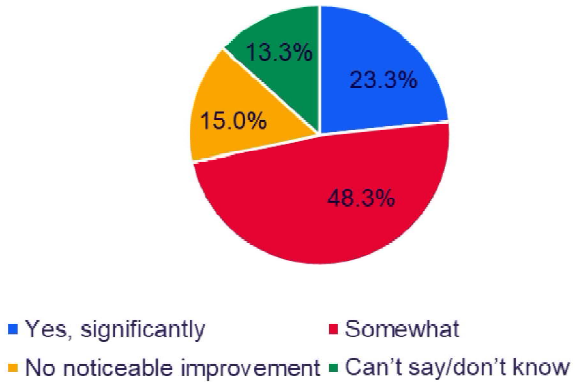
Figure 8: Concerns with AI (n=56 responses for 40 respondents)



Perceived Impact on Consumer Experience

Although AI adoption is widespread, its perceived benefits remain uneven. Of all the respondents, 23.3 percent reported that AI-based services had significantly improved their overall consumer experience, while 48.3 percent felt that the improvement was only to some extent. At the same time, 15 percent observed no noticeable improvement, and 13.3 percent were unsure or unable to assess the impact. These findings indicate that while a majority perceive some benefit from AI, its performance and value proposition do not consistently meet user expectations (Figure 9).

Figure 9: Impact on Consumer experience (n=60 responses for 60 respondents)

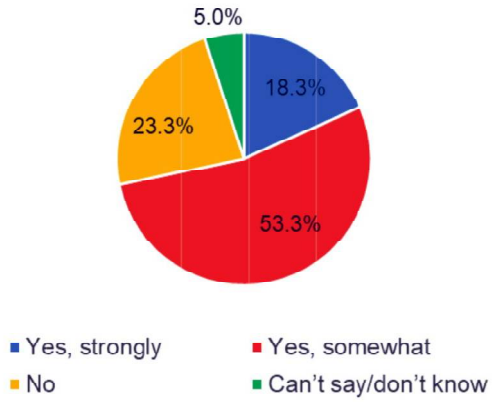


Influence of Personalised AI-Driven Advertisements and Recommendations

Personalised AI-driven advertisements and recommendations appear to have a moderate but uneven influence on consumer decision-making. A combined 41.6 percent of respondents acknowledged that such personalised content influenced their choices either strongly or to some extent. However, a majority that is, over half of the respondents (53.3 percent), reported that personalised recommendations did not influence their choices at all. A small proportion remained uncertain or unable to assess the impact.

These findings suggest that while algorithmic personalisation is effective for a significant segment of users, many consumers remain sceptical or consciously resistant to AI-driven nudging in digital environments such as e-commerce platforms, streaming services, and search engines (Figure 10).

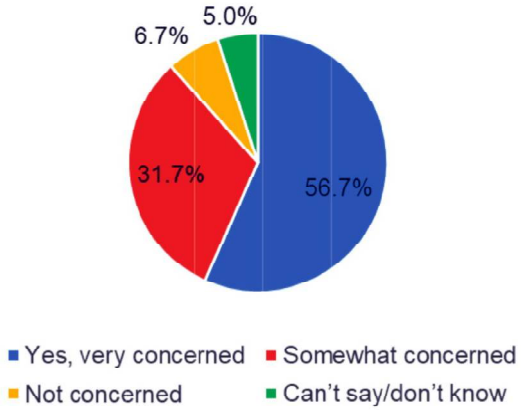
Figure 10: Influence of personalised AI-driven advertisements and recommendations (n=60 responses for 60 respondents)



Concerns Regarding Personal Data Handling by AI Tools

Concerns around personal data usage and privacy emerged as a prominent issue among respondents. An overwhelming majority expressed apprehension, with nearly one-third reporting that they were very concerned about how AI tools handle their personal data, and more than half indicating that they were somewhat concerned. Only a small fraction of respondents stated that they were not concerned, while a few were unsure. These results indicate a widespread trust deficit regarding data governance, transparency, and security practices of AI-powered services. Despite high levels of AI adoption, persistent anxiety over data misuse, surveillance, and a lack of user control remains a significant challenge for consumer trust (Figure 11).

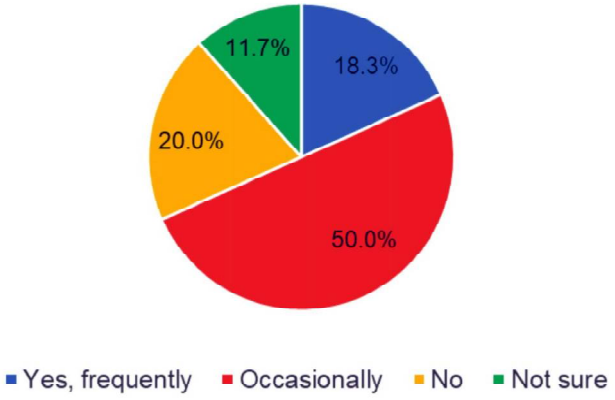
Figure 11: Consumer concerns about personal data handling by AI tools (n=60 responses for 60 respondents)



Challenges, Consumer Harm, and Trust Deficits

Difficulties in interacting with AI-driven services were widely reported. More than two-thirds of respondents (68.3 percent) indicated that they had faced problems either frequently or occasionally when engaging with AI-based systems such as chatbots, automated decision tools, or recommendation engines. One-fifth of respondents reported no difficulties, while a smaller proportion (11.7 percent) were unsure whether they had experienced any problems. The high incidence of reported issues suggests that challenges in AI interactions are not isolated but rather a common feature of consumer engagement with AI-enabled services (Figure 12).

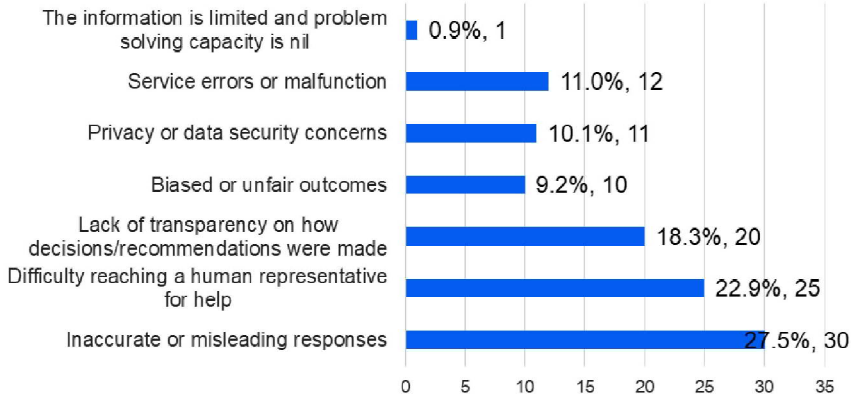
Figure 12: Difficulties faced with AI (n=60 responses for 60 respondents)



Among respondents who experienced difficulties, inaccurate or misleading responses emerged as the most significant concern, reported by nearly 70 percent of respondents. Difficulty in reaching a human representative was the second most common issue, affecting over half of the respondents, underscoring the limitations of AI systems in handling complex or non-standard queries. Nearly half of the respondents also cited a lack of transparency regarding how AI systems generate decisions or recommendations.

Additional concerns included service errors or technical malfunctions, privacy and data security risks, and biased or unfair outcomes, each affecting roughly one-quarter of respondents. A very small number of respondents highlighted the limited problem-solving capacity of AI systems, particularly in situations requiring contextual understanding or deviation from scripted responses. Overall, these findings point to systemic issues related to reliability, transparency, and accountability, which continue to undermine consumer trust in AI-driven services (Figure 13).

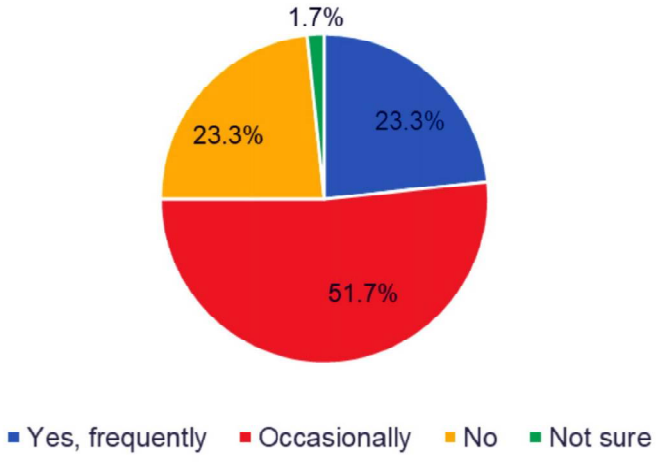
Figure 13: Type of problem faced with AI interaction (n=109 responses for 43 respondents)



AI-Based Customer Support and Grievance Redressal

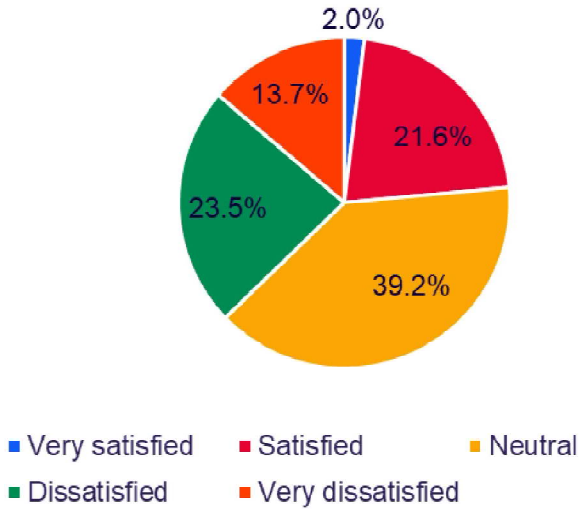
Interaction with AI-based customer support systems, including chatbots and automated support tools, was reported by a majority of respondents. Over half of the respondents (51.7 percent) indicated that they interacted with AI-based support occasionally, while 23.3 percent did so frequently. A similar proportion (23.3 percent) reported not interacting with AI-based support, and a very small fraction (1.7 percent) was unsure about this. These findings highlight that AI-based customer support has become a common point of consumer engagement, though it is not yet universally adopted (Figure 14).

Figure 14: Interaction with AI chatbots (n=60 responses for 60 respondents)



Among those who had interacted with AI-based customer support (n=51), satisfaction levels were generally low. Only 21.6 percent of respondents reported being very satisfied, and 13.7 percent were satisfied. A larger share of respondents was neutral (23.5 percent), while dissatisfaction was prominent: 39.2 percent of users reported being dissatisfied or very dissatisfied with the chatbot's ability to address their issues. These results suggest that while AI chatbots are widely used, their effectiveness in resolving consumer queries remains limited, emphasising the continued need for human oversight in customer support (Figure 15).

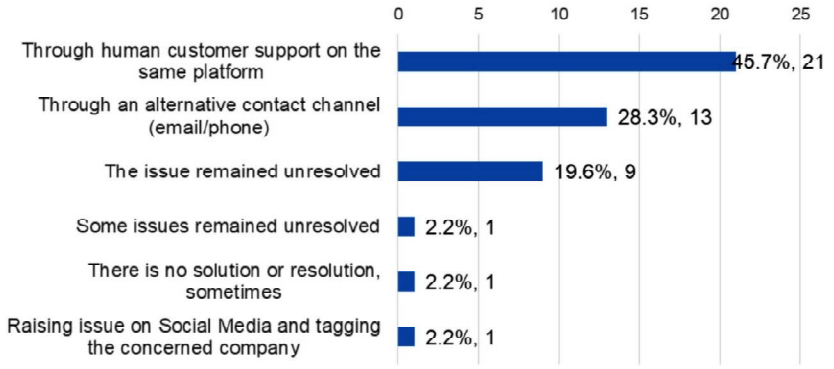
Figure 15: Satisfaction with AI chatbots (n=60 responses for 60 respondents)



For respondents who reported dissatisfaction or strong dissatisfaction with AI chatbots, issue resolution frequently required escalation beyond the automated system. More than half (58.3 percent) of dissatisfied respondents eventually received support through human customer service on the same platform. Others resorted to alternative communication channels, such as email or phone support (36.1 percent).

Notably, a quarter of respondents (25 percent) reported that their issues remained unresolved, with smaller fractions indicating partial resolution (2.8 percent), no resolution (2.8 percent), or resolving issues via social media engagement (2.8 percent). These findings underscore the limitations of AI-based support systems as standalone solutions and highlight the critical role of human intervention in ensuring effective grievance redressal (Figure 16).

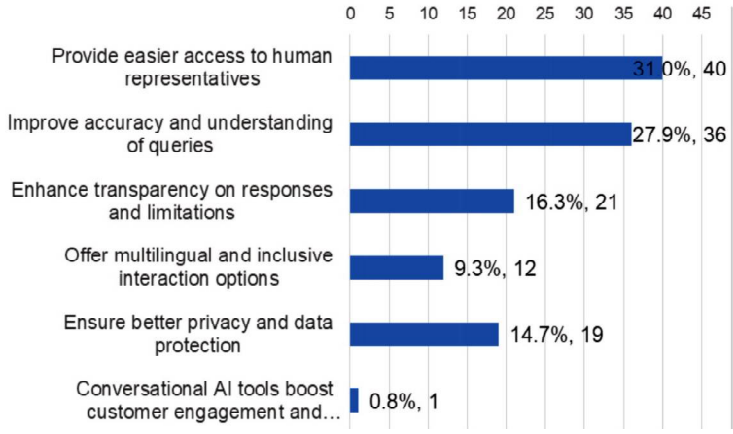
Figure 16: Resolution of issues after dissatisfaction with AI chatbots (n=46 responses for 36 respondents)



As regards to improvements needed in AI-based customer support chatbots, respondents overwhelmingly identified easier access to human representatives as the most critical improvement needed, followed by improved accuracy and greater transparency about system limitations. Other notable priorities included stronger privacy and data protection measures and multilingual or inclusive interaction options, indicating sensitivity to data security concerns and the diversity of India's linguistic landscape (Figure 15).

However, one respondent noted, "*Conversational AI tools boost customer engagement and satisfaction by offering fast, personalised responses and tailored solutions to customer needs. However, personalised responses may prove to be for such support systems has its own limitations.*" These findings suggest that its effectiveness is constrained unless reliability, transparency, inclusivity, and human fallback mechanisms are strengthened (Figure 17).

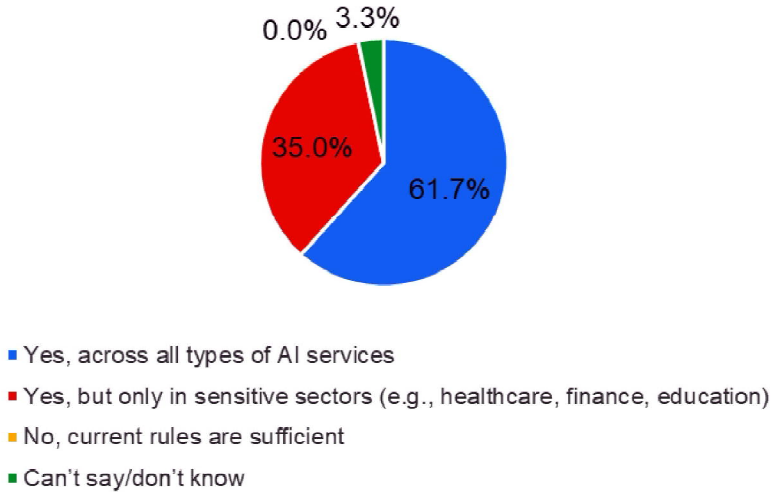
Figure 17: Improvements needed in AI based customer chatbots (n=129 responses for 60 respondents)



Demand for Regulatory Intervention

Support for government intervention in AI governance was strong and nearly unanimous. A majority of respondents favoured stricter regulation across all types of AI services, while others supported targeted regulation in sensitive sectors such as healthcare, finance, and education. Importantly, no respondent felt that existing regulatory frameworks were sufficient (Figure 18).

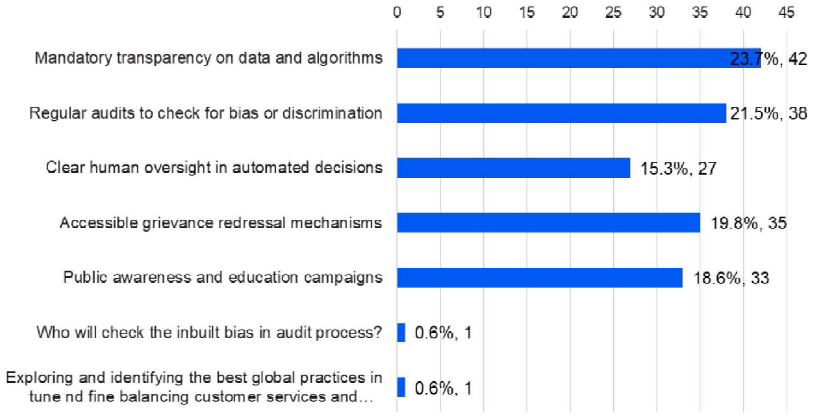
Figure 18: Regulation of AI and need for government intervention (n=60 responses for 60 respondents)



Respondents identified several priority measures for enhancing trust in AI systems. Mandatory transparency regarding data use and algorithms emerged as the most strongly supported measure, followed by regular audits to detect bias or discrimination. Accessible grievance redressal mechanisms, public awareness initiatives, and clear human oversight in automated decision-making were also widely endorsed. (Figure 17).

However, one participant even raised a question as to "*Who will check the inbuilt bias in the audit process?*" while another suggested that, "*Exploring and identifying the best global practices in tune and fine balancing customer services and preserving the ecosystem itself*" could be an approach. (Figure 19)

Figure 19: Measures to make AI more trustworthy (n=177 responses for 60 respondents)



Concluding Observations

The survey findings reveal a consumer landscape marked by growing engagement with AI-driven services alongside persistent concerns about accuracy, transparency, data protection, and accountability. While awareness of competition institutions such as the CCI is relatively high, understanding of regulatory roles remains incomplete, and perceptions of regulatory quality are cautious. For policymakers and regulators, these insights underscore the importance of integrating competition policy, consumer protection, and AI governance. Strengthening institutional capacity, improving public communication, and embedding consumer-centric safeguards into AI systems will be essential to ensuring that digital markets remain competitive, fair, and trustworthy.

As AI continues to reshape market dynamics and consumer interactions, regulatory responses must be informed by lived experiences and public expectations. This survey provides an evidence-based foundation for such policymaking, highlighting both the opportunities and the challenges of governing AI-driven markets in India.

While this chapter offers initial insights into consumer awareness and experiences with AI-powered services, its small, targeted sample provides only directional evidence. The findings highlight the importance of undertaking a larger, more representative survey to better understand diverse consumer experiences across India. Evidence from recent Indian consumer experience research shows that, despite widespread reliance on AI chatbots for service queries and complaint handling, significant challenges remain.

Many consumers continue to spend excessive time on hold, are repeatedly transferred between touchpoints, and report frustration with automated systems that fail to resolve issues efficiently, leading a large share of users to consider switching brands or leaving negative feedback online.[4]

Moreover, reports indicate that ineffective chatbot assistance is a major source of online shopping frustration in India, with a sizeable portion of consumers calling out poor chatbot performance when dealing with complex queries and highlighting the need for better integration with human support.[5]

The findings also point to systemic gaps in reliability, transparency, and accountability in AI applications, beyond just customer support chatbots. Strengthening grievance redressal mechanisms, improving algorithmic transparency, and ensuring clear human oversight emerge as critical priorities for enhancing consumer trust. Taken together, these findings underscore the need for a larger, more representative survey that examines broader AI adoption, perceptions, and concerns across the Indian consumer landscape to guide effective policy, regulation, and industry practices.

Endnotes

1 See Appendix 1 for the full survey questionnaire

2 Please see appendix 2 for the calculations.

3 *Ibid.*

4 https://www.livemint.com/companies/news/indian-consumers-spent-15-billion-hours-waiting-to-make-customer-service-complaint-in-2024-report-11742881208586.html

5 https://brandequity.economictimes.indiatimes.com/news/research/43-of-consumers-call-out-ineffective-chatbots-as-their-top-online-shopping-frustration-report/115898975

Appendix 1: Survey Questionnaire

Questionnaire – General (India Competition Perception Survey)

The country has been following a policy of market-oriented economic reforms for more than three decades. There is a need to assess the perception of the consumers about the competition and regulation regimes prevailing in the country and also on the quality of regulation.

In addition, with the rapid expansion of AI across sectors, it has become essential to understand how consumers perceive and experience the use of AI in their daily lives.

Accordingly, a questionnaire has been designed to get feedback from stakeholders on the following two broad issues:

- Awareness/knowledge regarding competition and regulatory issues
- Assessment of the level of competition and nature of practices that prevail in AI ecosystem

This survey will not take more than 10 minutes of your time. We thank you in advance for your valued cooperation and assure you of strict confidentiality. Neither your name nor the name of your organisation will be revealed in any document based on this survey.

Name: _____

Organisation: _____

Email: _____

I. General Awareness and Competition

1. Are you aware of the "Competition Commission of India"?

Yes	Go to Q2
No	Skip to Q5

2. Can you please tell the role/purpose of the Competition Commission of India? *(Select all that apply)*
   - To monitor competition of Stock Market
   - To promote competition in markets in India
   - To restrict inflow of FDI (Foreign Direct Investment)

- To investigate and adjudicate anti-competitive practices
- To monitor competition in distribution of FMCG/non-FMCG products
- To combat monopolistic trade practices
- Can't say/don't know
- Other:

3. How would you rate the quality of regulation in India?
   - Very Poor
   - Poor
   - Satisfactory
   - Good
   - Excellent

4. How can the quality of regulation be improved? Please rank these measures on a scale of 1-4 (choose 1, 2, 3 or 4) (1- lowest importance to 4 - highest importance)

By making regulatory bodies more independent
Allocating more budget
Good quality personnel
Reducing political interference

II. Artificial Intelligence (AI) Specific

5. Have you ever used or interacted with AI-powered services, including generative AI tools (e.g., ChatGPT), voice assistants, chatbots, etc?
   - Yes, frequently
   - Yes, occasionally
   - No
   - Don't Know/Not sure

6. Where do you most commonly encounter AI in your daily life? *(Select all that apply)*
   - Online shopping (e.g., product suggestions, dynamic pricing)
   - Streaming platforms (e.g., personalized movie or music recommendations)
   - Social media (e.g., curated content, filters, targeted ads)
   - Customer support (e.g., AI chatbots, automated phone systems)
   - Healthcare or fitness apps (e.g., symptom checkers, workout plans)
   - Generative AI tools (e.g., ChatGPT, DALL·E, AI writing assistants)
   - Workplace tools (e.g., AI for writing, data analysis, productivity)
   - Other (please specify): _____

7. Do you use multiple AI tools or platforms for similar purposes (e.g., using ChatGPT, Gemini, and Copilot together)?
   - Yes, regularly
   - Occasionally
   - No
   - Not sure

7a. (If Yes) What motivates you to use multiple AI tools? *(Select all that apply)*
   - Better accuracy or features
   - Comparison or verification of information
   - Privacy/security concerns
   - Free access limits or pricing differences
   - Others (please specify): _____

8. Do you feel that AI-based services, including generative AI, have improved your overall consumer experience?
   - Yes, significantly
   - Somewhat
   - No noticeable improvement
   - Can't say/don't know

9. Do you think personalised AI driven advertisements or recommendations on digital platforms (like e-commerce, streaming, or search engines) influence your choices?
   - Yes, strongly
   - Yes, somewhat
   - No
   - Can't say/don't know

10. Do you have concerns about how AI tools (including generative AI) handle your personal data, for example, when shopping online, using mobile apps, or interacting with digital assistants?
   - Yes, very concerned
   - Somewhat concerned
   - Not concerned
   - Can't say/don't know

11. Have you ever faced any problem or difficulty while interacting with AI-driven services (for example, chatbots, automated decision systems, or recommendation engines)?
   - Yes, frequently
   - Occasionally
   - No
   - Not sure

11a. (If Yes) What kind of problems have you faced? *(Select all that apply)*
- Inaccurate or misleading responses
- Difficulty reaching a human representative for help
- Lack of transparency on how decisions/recommendations were made
- Biased or unfair outcomes
- Privacy or data security concerns
- Service errors or malfunction
- Other (please specify): _____

12. Have you ever interacted with an AI-based customer support chatbots on an e-platform (such as online shopping sites, banks, telecom services, or government portals)?
- Yes, frequently
- Yes, occasionally
- No
- Can't say/Not sure

12a. If yes, how satisfied were you with the chatbot's ability to address your issue or query?
- Very satisfied
- Satisfied
- Neutral
- Dissatisfied
- Very dissatisfied

12b. If you were dissatisfied or very dissatisfied, how was your issue eventually resolved? *(Select all that apply)*
- Through human customer support on the same platform
- Through an alternative contact channel (email/phone)
- The issue remained unresolved
- Other (please specify): _____

13. In your view, what improvements are needed in AI-based customer support chatbots to serve consumers better? *(Select all that apply)*
- Provide easier access to human representatives
- Improve accuracy and understanding of queries
- Enhance transparency on responses and limitations
- Offer multilingual and inclusive interaction options
- Ensure better privacy and data protection
- Other (please specify): _____

14. In your opinion, should the government introduce stricter regulations to protect consumers from potential risks of AI and generative AI (such as misinformation, unfair targeting, or misuse of personal data)?
    - Yes, across all types of AI services
    - Yes, but only in sensitive sectors (e.g., healthcare, finance, education)
    - No, current rules are sufficient
    - Can't say/don't know

15. What measures do you think should be prioritised to make AI systems more trustworthy? (Select all that apply)
    - Mandatory transparency on data and algorithms
    - Regular audits to check for bias or discrimination
    - Clear human oversight in automated decisions
    - Accessible grievance redressal mechanisms
    - Public awareness and education campaigns
    - Other (please specify): _____

Appendix 2: Ranking Analysis of Measures to Improve Regulatory Quality

To determine respondents' priorities, we applied two complementary analyses:

1. Weighted Scoring (Borda Count)

   Each rank was assigned points according to the survey scale:
   Rank 1 = 1 point (lowest importance)
   Rank 2 = 2 points
   Rank 3 = 3 points
   Rank 4 = 4 points (highest importance)

   Total scores were calculated by multiplying the number of respondents assigning each rank by the corresponding points and summing across ranks.

2. Top-Rank Percentage

   The proportion of respondents ranking each measure as Rank 4 (highest importance) was calculated to identify which measure was most frequently selected as the single top priority.

Results

Measure Rank ***(sorted by weighted score)***	**Rank 1**	**Rank 2**	**Rank 3**	**Rank 4**	**Weighted Score (** Σ ***[Rank/Point× Number of respondents])***	**percent Top-Votes** ***(Rank 4 ×100÷60)***
Good quality personnel	10	12	20	18	166	30 percent
Independence of regulatory bodies	12	16	15	17	157	28.3 percent
Reducing political interference	17	10	12	21	157	35 percent
Allocating more budget	21	22	13	4	120	6.7 percent

CHAPTER 3

Emerging Competition Issues in AI

Introduction

AI is transforming the global economy at an unprecedented pace, with 78 percent of companies worldwide already integrating AI into at least one business function as of 2025[1] and global AI market expected to reach US$1.85tn by 2030.[2]

This widespread adoption went up from just 20 percent in 2017[3] to 78 percent in 2025, this dramatic adoption of AI reflects AI's transition from being a niche technology to a mainstream business tool driving productivity, innovation, and digital transformation. Generative AI models, recommendation engines, autonomous systems, and predictive analytics are increasingly reshaping how businesses compete and operate, influencing not only economic outcomes but also market structures.

While AI driven advancements foster innovation and growth, they may also risk distorting competition and increasing market concertation. AI markets are characterised by intense data requirements, where vast, high-quality datasets concentrated among a few firms create significant entry barriers leading to data-driven market power. But as AI grows in sophistication, it also introduces a set of unique challenges for market competition.

Unlike traditional industries, AI markets are often dominated by a few firms with access to vast amounts of data, specialised computing infrastructure like Graphics Processing Unit (GPUs) and Tensor Processing Unit (TPUs), and advanced cloud resources. This combination creates significant barriers for smaller players, making it difficult for them to compete on equal footing.

The competitive advantage in AI often stems from network effects and feedback loops. The more users interact with a platform, the more data it generates, improving the performance of AI models and enhancing the user experience.

This chapter has been contributed by Vishi Maharishi, Junior Consultant, CUTS International.

This dynamic accelerates the dominance of early movers and reinforces "winner-takes-most" outcomes, as observed in the current digital ecosystem, where a handful of tech giants control the majority of data and reap the corresponding benefits. Yet, while data fuels innovation, it also opens the door to potential market abuses.

Algorithms can be leveraged to engage in collusion, manipulate prices based on user behaviour, favour a firm's own products over competitors, or deploy predatory pricing strategies. Large-scale AI models, especially generative models, often operate as "black boxes," making it challenging to detect anti-competitive conduct or abuse of market power.

Recognising these complexities, authorities around the world, including in India, are actively adapting legal frameworks and policy tools. Beyond traditional antitrust approaches, policy makers are exploring AI-specific safeguards, such as the European Union's AI Act, aimed at ensuring AI technologies are used responsibly without stifling innovation. Understanding AI's multifaceted impact on competition is crucial for policymakers and regulators. This chapter explores AI markets and the competition challenges they pose in today's economy.

Competition Law Issues in AI Markets

Defining a Market and Power Assessment

Defining a market is a crucial first step in competition law analysis, as it helps identify the boundaries within which firms operate and compete. By establishing the *relevant market*, authorities can assess an enterprise's market share, degree of dominance, and the competitive constraints it faces. In essence, market definition provides the framework for determining whether certain conduct may have an anti-competitive effect.

Traditionally, market definition has relied heavily on price-based analysis. Tools like the SSNIP test (Small but Significant and Non-Transitory Increase in Price) are used to assess demand substitutability, that is, whether consumers would switch to another product or service if the price of one increased slightly. This analysis lies at the heart of identifying the relevant market. However, in digital markets, where many services are offered at zero monetary price (for example, social media platforms, search engines, or email services), the role of "price" as a determinant has become largely obsolete.

The Organisation for Economic Co-operation and Development (OECD) 2018 report[4] also observed that it makes little sense to consider a price increase on a side of the market where the price is zero to begin with.

As Newman[5] pointed out, transactions in digital markets still resemble traditional buyer-seller exchanges as firms provide zero-priced products in exchange for users' attention or personal data. This dynamic reflects the well-known observation from Serra and Schoolman's 1973 film "If you are not paying for the product, then you are the product." Consequently, competition in these markets often takes place not on price, but on dimensions such as quality, innovation, privacy standards and user experience all while being driven by the underlying incentive to collect and monetize user data.

To capture this shift, competition authorities have begun exploring alternative tests such as the SSNDQ test (Small but Significant and Non-Transitory Decrease in Quality). The SSNDQ test examines whether a small but sustained reduction in the quality of a product or service would cause users to switch to another provider. If users would switch in response to a decrease in quality, then those alternatives are considered part of the same relevant market. This approach helps assess non-price competition in digital ecosystems.

While the SSNDQ test provides a more realistic lens for analysing competition in digital markets, it also poses challenges. Unlike price, quality is inherently subjective and may vary based on user preferences or product characteristics. This makes it difficult to establish a uniform benchmark for assessing what constitutes a significant change in quality. Moreover, firms may not always have sufficient data or analytical tools to conduct a robust SSNDQ assessment. Additionally, many digital platforms operate as multi-sided markets, serving different groups of users simultaneously (e.g., advertisers and consumers).[6] This interdependence further complicates market definition, as changes on one side of the platform can affect competitive dynamics on the other.

In 2019, CUTS International did a primary study on relevant market in the ride-sharing industry in the Delhi-NCR region, applying SSNIP and SSNDQ framework.[7] The findings suggested that both the test are not substitutes of each other. Hence, it would be inappropriate for regulators to use SSNIP as a substitute in digital platform contexts, as each test focuses on distinct assessment criteria and can yield different market definitions. This distinction is particularly important for regulators in digital and AI-driven markets, which are highly dynamic and rapidly evolving.

In sum, while traditional price-based tools like SSNIP have been central to defining markets, the rise of digital, data-driven, and zero-price ecosystems has prompted the need for qualitative, multi-dimensional approaches like using combination of the SSNDQ and SSNIP test is more appropriate to capture the true nature of competition in modern markets.

Data and Input Bottlenecks

In the AI economy, *data itself has become the strongest form of lock-in.* What once served merely as an input for innovation now functions as a mechanism of control binding users, developers, and even competitors to dominant platforms. While regulators often advocate for data portability as a tool to enhance competition, its effectiveness remains limited.

The problem lies in what kind of data can actually be ported. Users may be able to transfer their raw inputs like files, images, or records but not the richer layers of *inferred* or *derived* data that platforms generate through analytics, model training, and user interactions. These hidden layers hold the real value, and they stay locked within the incumbent's ecosystem. Even with legal rights to move "their" data, cannot replicate the underlying intelligence or predictive power that the platform has accumulated over years of operation.[8]

This asymmetry creates a subtle but powerful dependency. As firms integrate more deeply with an AI vendor using its Application Programming Interfaces (APIs), cloud tools, or proprietary model architectures the costs of switching rise dramatically. These dependencies form across multiple layers: data formats, infrastructure, APIs, and model fine-tuning.[9]

What makes data-driven lock-in especially pernicious is its invisibility. Unlike traditional contractual or pricing lock-ins, data lock-in operates quietly in the background. Every interaction generates new information that feeds back into the platform's learning systems, deepening its advantage while making the user increasingly dependent. The more data a firm accumulates, the more personalised and efficient its services become and the harder it is for users or smaller competitors to replicate that value elsewhere.

This creates a form of *structural inertia*[10] in digital markets, where innovation is stifled not by explicit exclusion, but by the sheer gravitational pull of accumulated data. In essence, data has evolved from a competitive asset into a competitive moat one that is nearly impossible to cross without regulatory intervention or systemic change.

AI-Induced Cartels

The digital economy is rewriting the rules of competition. As pricing algorithms learn to adapt, match, and even anticipate competitors' strategies, they may end up fixing prices without a single word exchanged between rivals. Price fixing agreements have historically been through explicit human-led collusion between the competitors which primarily aimed to manipulate the market dynamics and maximise the profit by undermining consumer

choice. AI is increasingly being integrated by businesses to improve on their business operations.

According to recent market study by Competition Commission of India (CCI) on AI and competition law, 90 percent business has already integrated AI to monitor customer behaviour and about 69 percent of respondents rely on AI for demand forecasting.[11]

AI's capabilities like machine learning, pattern recognition, predictive analysis and reinforcement learning can be used to absorb large amounts of data and make decisions based on that data. Use of AI improves business efficiency but can also be used as a gateway to potential collusions such as price fixing. This new frontier of algorithmic collusion poses unprecedented challenges for antitrust enforcement.

In context of AI, cartel like behaviour between competitors generally manifest through algorithmic collusions. AI has automated the process of streamline communication. This is primarily done by machine learning performed by AI, which mimics patterns of how our brain works. The basic building block is called a "perceptron,"[12] similar to a brain cell. It takes in data, processes it, and sends out a result. These perceptron's are connected, and the connections can be adjusted based on how well the system is performing.

Further, the accuracy of this analysis increases with the amount of data that is fed into the system. Unlike traditional cartels, which rely on human agreement and enforcement, algorithmic collusion involves firms deploying pricing algorithms that interact in the marketplace.

Challenges of Establishing Collusion in AI-Driven Markets

Unlike traditional cartels, most of the AI driven cartels operate without human intervention which makes it difficult to assess the liability of algorithms. In the Las Vegas Strip case[13], the federal judge dismissed the case primarily as there was no of "meeting of minds" and lack of evidence to substantiate the existence of a cartel either explicitly or tactically. The algorithms were used at different times and the plaintiff was unable to show exchange of any confidential information between the players. This is one of the main challenges when it comes to AI driven cartels.

AI driven algorithms can make autonomous decisions without the need of human interventions; as, the present legal structure rely on intent and existence of some agreement between the parties with some human intervention. Hence, it is difficult to pin down the blurry line between legal and illegal use of these AI driven algorithms.

In India, the very first case discussing algorithmic collusion was *Samir Agarwal vs ANI Technologies,*[14] wherein it was alleged that taxi aggregator (Uber and Ola) used algorithms to engage in hub and spoke cartel, CCI dismissed the case explicitly denying that merely algorithmic determined prices will not be enough to constitute an "agreement". However, CCI has since moved from denial to acknowledgement[15] of AI driven collusions.

In the recent case of *Shikha Roy v Jet Airways*[16], it was alleged that airlines charged excessive fares due to possible algorithmic collusion. While CCI did acknowledged the possibility of algorithmic collusions, it found no explicit evidence of "agreement" or tactic collusion. CCI noted that the airlines used different pricing software and the final call for inventory allocation was taken by independent route analyst of airlines. Therefore, owing to insufficient evidence CCI did not find any violation of the Competition Act.

The current regulatory landscape reveals a significant enforcement gap when "accidental" collusion might occur through algorithmic coordination. Liability under Section 3 requires the presence of a direct or inferred agreement, which becomes difficult to establish when black-box algorithms produce collusive outcomes without any traceable human intent or communication. To address the said concern, authorities can potentially shift from a form based to an effect-based assessment (which has also been affirmed by recent Supreme court Schott Glass case).

However, it can also be argued that algorithmic coordination may not always amount to cartelisation, particularly when pricing algorithms operate based on publicly available market information rather than any concealed exchange or communication among competitors. In such cases, algorithms are merely reacting to the competitive environment scraping, analysing, and adjusting prices derived from already published data. This behaviour could, in theory, be viewed as an extension of ordinary market efficiency rather than a manifestation of collusion.

After all, one of the hallmarks of competitive markets is responsiveness: firms continuously monitor rivals' prices to remain competitive, and algorithms simply enable this process to occur at a far greater speed and precision. Therefore, the challenge for competition law lies in developing nuanced standards capable of distinguishing algorithmic efficiency from algorithmic coordination. This may involve greater scrutiny of the algorithm's design whether it merely optimises prices individually or embeds interdependent parameters that predict competitors' moves. Ultimately, not every instance of algorithmic price alignment should be condemned as collusion; some may indeed represent the new face of competitive efficiency in digital markets.

Abuse of Dominance

Exclusionary Conduct

i. Tying and Bundling

A tying arrangement occurs when a seller conditions the purchase of one product on the buyer also purchasing another, "tied" product.[17] The main concern with tying is that it can limit goods from competing independently, preventing consumers from making choices solely based on the merits of each product. Bundling, which involves selling products together at a combined price, can be structured in different ways, such as pure bundling or mixed bundling with discounted rates.

In the context of AI, major platforms often integrate AI tools or applications into their core products like search engines, browsers, operating systems, or cloud services. While this can accelerate adoption and improve user experience, it may also make it more challenging for smaller competitors to enter the market. For instance, cloud providers may bundle AI models with their cloud services, and telecom companies may pair AI-powered assistants or search tools with traditional services, as seen in partnerships like Airtel and Perplexity.[18]

Similarly, hardware companies integrate AI into their devices, such as Apple embedding Apple Intelligence in its devices with optional ChatGPT integration, or Microsoft incorporating ChatGPT into Windows and PCs via Copilot.[19] While these bundles enhance functionality for users, they may subtly influence consumer choice, as many users opt for the default integrated option. Switching to alternative platforms can involve non-monetary costs, such as the effort to learn new systems or transfer data, which reinforces the presence of established players in the market.

ii. Self-Preferencing

Self-preferencing is understood as an enterprise with market power favouring its own products and services over those of its rival competitors.[20] A key concern is AI-driven self-preferencing, where platforms use algorithms to favour their own services over competitors. CCI in the recent market study noted that dominant enterprises may leverage market power to promote and self-prefer their own products which can reinforce their position in the market and also be capable of being an entry barrier for smaller players.

Following this, it is important to understand the manifestation of self-preferencing in digital markets and AI-driven ecosystems. In digital markets, self-preferencing often occurs when dominant platforms such as online marketplaces, app stores, or search engines use their control over algorithms, data, or user interfaces to give preference to their own products or services. This could include ranking their own offerings higher in search results,

giving preferential visibility to their own applications, or using data collected from third-party competitors to improve their own products.

In the context of AI, self-preferencing takes a more complex and opaque form. AI systems, particularly those powered by machine learning and recommendation algorithms, can subtly bias outcomes in favour of the platform's own interests. For instance, an AI-powered recommendation engine could be trained or optimised to systematically prioritise the platform's proprietary content or services under the guise of "relevance" or "user benefit." Such practices are difficult to detect, as algorithmic decision-making lacks transparency and can be justified under technical optimisation parameters.

Consequently, AI-driven self-preferencing not only distorts competition but also raises regulatory concerns around fairness, accountability, and explainability. It may entrench dominant positions, limit consumer choice, and create data-driven feedback loops where the dominant firm's access to larger datasets further enhances its AI performance, deepening competitive asymmetries in the market.

A key example is the 2017 European Commission case against Google, where the company was fined €2.42 billion for promoting its own comparison-shopping service over rivals. The General Court (2021) upheld this decision, confirming that self-preferencing can amount to a standalone abuse of dominance when it produces anticompetitive effects and departs from competition on the merits. This case underlines how such conduct, especially when driven by AI algorithms, can reinforce dominance and hinder fair competition in digital markets.

iii. Refusal to Deal

As per Competition Act 2002, refusal to deal includes any agreement which restricts, or is likely to restrict, by any method the persons or classes of persons to whom goods are sold or from whom goods are bought.[21] The refusal to deal is not problematic or anticompetitive *per se*, business have the right to deal with the enterprises they choose; however, it becomes problematic when such "refusal" affects the competition in the market.

Such cases only happen when the enterprise provides an 'essential' facility. Under EU framework, refusal to deal constitutes abuse of dominance when a dominant firm denies access to an indispensable input. The landmark Oscar Bronner case[22] established three conditions: (i) refusal likely eliminates all competition, (ii) refusal lacks objective justification, and (iii) the input is indispensable, meaning no actual or potential substitute exists.

EC's Microsoft decision[23] exemplifies strict application: Microsoft, with 95 percent market share, was found to have breached Article 82 EC by refusing to supply interoperability information to rivals, thereby foreclosing competition. Similarly, in Slovak Telekom, the CJEU clarified that the Bronner test applies only to outright refusals. Implicit refusals such as imposing unfair conditions or delays may constitute abuse even without proof of indispensability.

Turning to the context of artificial intelligence and digital markets, data now functions as the key input driving competitiveness and innovation. Denying access to essential datasets could therefore exclude market players, entrench dominant positions, and create barriers to entry. While the CCI has not yet classified data as an essential facility, it has, in several cases,[24] acknowledged that data can raise significant competition concerns. However, demonstrating that data is truly "indispensable" poses unique regulatory challenges.

Unlike physical infrastructure such as railways or telecom networks, data is non-rivalrous, abundant, and often substitutable. This makes it far more difficult to prove that access to a particular dataset is indispensable for effective competition in digital markets.

Firstly, it would be difficult to prove that data is truly indispensable, given its abundance and substitutability. *Secondly,* forcing firms to share data might undermine their incentives to invest in data collection, AI model training, and technological innovation. *Thirdly*, digital markets are highly dynamic, and over-regulation could stifle innovation, which in turn promotes competition. Moreover, multi-homing and data portability where users interact with multiple platforms and share data across them—further weaken the argument that a single dataset is essential.

Finally, there is a risk of regulatory overreach, as prematurely classifying data as an essential facility could impose disproportionate obligations and hinder digital growth, particularly in developing economies like India. In shaping regulation for digital markets, a cautious and balanced approach may be more effective than sweeping interventions. Regulators could consider a case-by-case approach to indispensability, assessing whether access to data or AI is truly essential in a given context.

Exploitative Conduct

i. Excessive Pricing and Price Discrimination

Article 102(c) of the Treaty on the Functioning of the European Union (TFEU) defines price discrimination as "*applying dissimilar conditions to equivalent transactions with other trading parties, thereby placing them at a competitive disadvantage.*" While the principle seems straightforward, it raises an enduring

question: why is price discrimination considered anticompetitive when, in many cases, it appears to be just another pricing strategy?

From economic perspective, price discrimination is common and widespread used across industries to stimulate sales, recover fixed costs, and increase profits.[25] As Bergqvist and Marinova,[26] such practices are not inherently anticompetitive and often occur even in competitive markets such as airlines, cinemas, or transport. They allow firms to serve consumers with different willingness to pay, expanding output and improving cost recovery. From a welfare perspective, discrimination may increase efficiency when it enables access for more price-sensitive consumers.

However, what distinguishes legitimate pricing strategies from abusive discrimination under Article 102(c) TFEU lies in fairness and transparency. When similar buyers are treated differently for reasons unrelated to cost or efficiency, competition and consumer trust are both undermined.

The Schott Glass judgment[27] reaffirmed that not all discriminations are unlawful. Volume or functional discounts, if applied transparently and on equal terms, are permissible, what matters is whether there is an adverse effect on competition or not. Yet the digital marketplace challenges these principles. Here, price discrimination is increasingly powered by AI and big data, which allow sellers to personalise prices for each user based on individual data traces search history, device type, location, or even purchase timing.

Such algorithmic price discrimination makes what economists once called "first-degree discrimination" operationally feasible for the first time.[28] Algorithms can segment consumers with remarkable precision, predict willingness to pay, and prevent arbitrage through digital design non-transferable accounts, geo-blocking, or digital rights management. In short, the very conditions that once made perfect price discrimination impossible now exist online through AI.

The result is a form of invisible sorting where consumers are charged different prices for identical products under identical conditions, often without ever realizing it. The harm is not only monetary it is procedural, embedded in the opaque process through which prices are determined. Consumers are deprived of agency, their autonomy eroded by algorithmic profiling that exploits behavioural biases and information asymmetries.

A recent study in *Marketing Science* by researchers at Carnegie Mellon University strengthens this concern.[29] It shows that even in the absence of explicit price discrimination, personalised product rankings can reduce price competition. By ranking products in order of predicted consumer utility,

platforms reduce users' price sensitivity and thereby enable higher prices. This ranking-mediated elasticity effectively dampens the competitive process consumers click what they see first, not what is cheapest.

These dynamics harm not only consumers but also market contestability. Over time, algorithmic pricing becomes not just a revenue tool but a barrier to entry, entrenching dominance and marginalising smaller competitors.

From the U.S. perspective, these practices echo the concerns underlying the Robinson–Patman Act, which prohibits discriminatory pricing that injures competition or grants unfair advantages among purchasers of like goods. While U.S. enforcement historically declined, the Federal Trade Commission (FTC) has recently revived scrutiny of discriminatory pricing in digital markets, especially where algorithmic systems result in systematic disparities that distort competition. The FTC's guidance reminds firms that "charging different prices to different buyers for the same goods may violate the law when it lessens competition or injures consumers."[30]

What makes AI-driven discrimination uniquely problematic is its invisibility. Traditional price differences say, between wholesale and retail, or bulk and individual buyers are visible, explainable, and often rational. Algorithmic pricing, by contrast, operates in the dark; it is neither observable by consumers nor easily verifiable by regulators. As Bergqvist and Marinova argue, the harm lies not necessarily in *price level*, but in the *process* where opaque, data-driven systems manipulate individual perception and extract surplus without transparency or justification.[31]

Moreover, the behavioural dimension cannot be ignored. Studies show that consumers perceive price discrimination as unfair when they cannot understand or anticipate why they pay more than others.[32] Fairness concerns directly affect trust and willingness to transact. When consumers suspect that personal data is being used to disadvantage them, welfare falls even if total market efficiency rises. In this sense, algorithmic discrimination transforms "personalisation" from a feature into a form of digital exploitation.

In conclusion, price discrimination may have long served as a legitimate tool to stimulate sales and enhance efficiency, but in the algorithmic age, it risks crossing a line. When data becomes the new market power and algorithms learn to exploit every micro-preference, efficiency no longer guarantees fairness. The invisible calculus of AI-driven pricing threatens not only to drain consumer surplus but to erode competition itself transforming the promise of personalisation into a system of quiet, perpetual inequity.

Mergers and Acquisitions

i. Killer Acquisitions

The term "killer acquisition" is not formally defined in competition law, but it generally describes a situation in which a dominant or established firm acquires a smaller, emerging competitor before it can evolve into a meaningful market rival. Such acquisitions are often driven not by the objective of scaling or integrating innovation, but by the strategic intent to neutralise a potential competitive threat to the incumbent's market position. The concept first gained prominence in the pharmaceutical sector, where large firms frequently acquired smaller biotech companies developing novel molecules or treatments, sometimes with no intention of commercialising them, but rather to protect the profitability of their existing patented products.

A classic example of a killer acquisition is Facebook's 2012 purchase of Instagram. At the time, Instagram was a young but fast-growing photo-sharing app that posed no immediate competitive (and financial) threat to Facebook. It had the potential to divert user attention and advertising revenue both vital to Facebook's core business model. By acquiring Instagram early, Facebook pre-empted this competitive risk and consolidated its dominance in the social media ecosystem.

These transactions often fall outside the scope of traditional merger control regimes, because the target firm has limited turnover or assets that does not trigger notification thresholds. Nevertheless, their potential competitive harm can be substantial, as they may eliminate future competition before it materialises. In this context, incorporating deal value–based thresholds as an additional jurisdictional trigger has emerged as a potential regulatory tool. Such an approach could act as a safeguard against killer acquisitions, particularly in the AI ecosystem, where start-ups may have low revenues but high strategic value due to data, technology, or innovation potential.

From competition point of view, killer acquisitions disrupt, what Joseph Schumpeter described as the process of creative destruction, the natural cycle through which new and innovative firms challenge incumbents, forcing markets to evolve.[33] When incumbents buy and bury potential challengers, they arrest this process, concentrating power and stifling innovation.

This concern has become particularly acute in the AI market, where the logic of competition hinges on access to data, computing power, and talent. In AI, the big tech typically enjoys a decisive competitive advantage, it can train more effective models, attract more users, and in turn, collect even more data, reinforcing a self-perpetuating cycle of dominance. Against this backdrop, big technology firms across the globe have been on an acquisition spree, buying promising AI startups even before they pose any visible threat.

Google's acquisition history illustrates this vividly with purchases like DeepMind, API.ai, Alooma, AppSheet, and Fitbit, among others.[34] While some of these deals have undoubtedly strengthened Google's AI ecosystem, they also highlight how early-stage takeovers can remove future competitors from the market. Google, however, is not alone. Other tech giants such as Microsoft, Amazon, and Meta have also been actively acquiring AI firms, often integrating their technologies into existing systems while eliminating independent avenues for innovation.

Yet, the narrative around killer acquisitions is not entirely one-sided. In certain sectors, particularly pharmaceuticals, acquisitions can play a constructive role. Start-ups often innovate with an exit in mind, developing products intended to be acquired by larger firms that possess the capital and infrastructure necessary for large-scale trials, regulatory approval, and distribution. In such cases, acquisitions may facilitate rather than suppress innovation. The real challenge lies in distinguishing transactions that enable innovation from those that eliminate future competitive threats.

From an enforcement perspective, existing merger control frameworks struggle to capture this distinction. Traditional notification thresholds, largely based on turnover or asset value, frequently fail to detect acquisitions of high-potential start-ups with minimal current revenues. As a result, many killer acquisitions escape scrutiny, creating a serious enforcement gap. By the time competitive harm becomes visible, the target's independent incentives and innovative capacity have often already been irreversibly absorbed or extinguished.

In response, deal value–based notification thresholds have emerged as a potential safeguard. By focusing on the strategic value of a transaction rather than the target's present turnover, such thresholds can alert authorities to acquisitions that may remove future competitive constraints, particularly in innovation-driven sectors such as AI. Without a more forward-looking enforcement approach, market dynamics risk entrenching a small number of dominant digital firms focused on optimizing existing revenue streams rather than pursuing transformative innovation.

Conclusion and Way Forward

AI is transforming competitive dynamics across markets by generating new efficiencies while simultaneously amplifying risks of concentration, exclusion, and algorithmic collusion. Traditional competition law frameworks, which are largely grounded in assumptions of human-led decision-making, often struggle to address challenges arising from data dependence, algorithmic opacity, and autonomous pricing or coordination mechanisms.

To ensure that AI-driven innovation remains pro-competitive, regulators must adopt a forward-looking, effects-based enforcement approach. Strengthening institutional capacity within the CCI to assess algorithmic and data-driven practices is therefore essential. A positive step in this direction is the establishment of the Digital Markets Division within the CCI, which is mandated to build internal expertise on digital markets, data-related conduct, and emerging technologies, thereby enabling more informed and timely competition assessments in technology-intensive sectors.

Further, clear regulatory guidance on AI-related conduct such as data sharing arrangements, transparency obligations, and accountability for algorithmic outcomes can help bridge existing enforcement gaps. The CCI's Market Study on AI provides a constructive example in this regard. The study systematically maps AI value chains, identifies competition risks such as data concentration and self-preferencing, and highlights the need for adaptive enforcement tools, offering early guidance without stifling innovation.

Recent international[35] developments reinforce the need for such proactive oversight. For instance, the European Union's launch of an antitrust probe into Meta concerning the use of AI trained on WhatsApp data underscores how competition authorities globally are increasingly scrutinising AI-related conduct even in the absence of traditional price effects. Such actions demonstrate a willingness to intervene at an early stage where data and AI capabilities risk entrenching market power.

Ultimately, a coordinated policy approach involving competition law, data protection, and broader digital governance frameworks will be critical to maintaining fair and contestable AI markets. India's competition regime must proactively encourage responsible AI innovation while deterring practices that entrench dominance or undermine consumer welfare. The overarching objective should be to ensure that AI serves as a driver of inclusive growth and fair competition, rather than a catalyst for digital monopolisation.

Endnotes

1 https://www.mckinsey.com/capabilities/quantumblack/our-insights/the-state-of-ai.

2 https://explodingtopics.com/blog/companies-using-ai.

3 Id.

4 https://www.oecd.org/content/dam/oecd/en/publications/reports/2018/10/digital-trade-and-market-openness_60f04c17/1bd89c9a-en.pdf.

5 https://www.thefreelibrary.com/Antitrust+in+zero-price+markets percent3A+foundations.-a0442286320

6 https://digitalregulation.org/approach-to-market-definition-in-a-digital-platform-environment/.

7 evidence-based-analysis-the-case-of-ride-sharing-in-delhi-national-capital-region.pdf.

8 https://jolt.law.harvard.edu/assets/articlePDFs/v36/Zhang-The-Paradox-of-Data-Portability-and-Lock-In-Effects.pdf.

9 https://ctomagazine.com/ai-vendor-lock-in-cto-strategy/

10 Structural inertia is the tendency of an organisation or system to resist change and maintain its existing structure, even when external pressures or internal inefficiencies suggest change is needed.

11 https://www.cci.gov.in/economics-research/market-studies/details/47/0.

12 https://link.springer.com/article/10.1007/s40319-018-00773-x.

13 https://business.cch.com/ald/GibsonvCendynGroupLLC592024.pdf.

14 https://www.cci.gov.in/images/antitrustorder/en/3720181652328966.pdf.

15 https://awards.concurrences.com/IMG/pdf/shikha_roy_v_jet_airways-a_new_approach_to_algorithmic_collusion-afif_and_shifa.pdf?103009/b0aab30d515eafc4f2085f6e0bd0cdb5169a4e3a4bba73f3bc304d2c4e62f1a8#:~:text=On percent 203 percent20June percent2C percent202021 percent2C percent20the,of percent20air percent20tickets percent20because percent20of.

16 https://www.cci.gov.in/antitrust/orders/details/33/0.

17 *Jefferson Parish*, 466 U.S. at 22.

18 https://indianexpress.com/article/technology/techook/airtel-perplexity-pro-free-annual-subscription-how-to-claim-10131852/.

19 https://businesslawreview.uchicago.edu/online-archive/potential-antitrust-implications-tying-hardware-ai.

20 Market study AI CCI.

21 Explanation (d), Section 3(4), Competition Act, 2002.

22 https://www.europeanpapers.eu/e-journal/landmark-judgment-in-refusal-to-deal-doctrine-android-auto-and-bronner-future-in-digital-platform-markets

23 https://competition-cases.ec.europa.eu/cases/AT.37792

24 Matrimony.com vs CCI

25 https://www.konkurrensverket.se/globalassets/dokument/informationsmaterial/rapporter-och-broschyrer/pros-and-cons/rapport_pros-and-cons_2005_the-pros-and-cons-of-price-discrimination.pdf.

26 https://papers.ssrn.com/sol3/papers.cfm?abstract_id=5153695.

27 https://api.sci.gov.in/supremecourt/2014/19707/19707_2014_5_1501_61745_Judgement_13-May-2025.pdf.

28 https://ia903405.us.archive.org/20/items/in.ernet.dli.2015.166890/2015.166890.The-Theory-Of-Price.pdf.

29 https://www.cmu.edu/tepper/news/stories/2025/0602-ai-driven-personalized-pricing-may-not-help-consumers.

30 https://www.ftc.gov/advice-guidance/competition-guidance/guide-antitrust-laws/price-discrimination-robinson-patman-violations.

31 https://papers.ssrn.com/sol3/papers.cfm?abstract_id=5153695.

32 Priester, A., Robbert, T. & Roth, S. A special price just for you: effects of personalized dynamic pricing on consumer fairness perceptions. *J Revenue Pricing Manag* **19**, 99–112 (2020). https://doi.org/10.1057/s41272-019-00224-3

33 https://www.promarket.org/2025/05/27/we-must-avoid-killer-acquisitions-at-the-birth-of-ai/.

34 https://moginlawllp.com/big-techs-decade-of-a-i-shopping/.

35 https://ec.europa.eu/commission/presscorner/detail/en/ip_25_2896.

CHAPTER 4

Artificial Intelligence and Tacit Collusion: An Indian Competition Law Perspective

Introduction

Collusion is legal when the process by which it is achieved is legal. One such category is conscious parallelism, which is the process "not in itself unlawful, by which firms in a concentrated market might, in effect, share monopoly power, setting their prices at a profit-maximising, supra-competitive level by recognising their shared economic interests[1]." Along these lines, Judge Posner commented that "*it is not a violation of antitrust law for a firm to raise its price, counting on its competitors to do likewise (but without any communication with them on the subject) and fearing the consequences if they do not.*"[2]

Tacit collusion, as the name suggests, is an agreement that is implied or indicated, but not explicitly stated.[3] It refers to forms of anti-competitive coordination which can be achieved without any need for an explicit agreement, but which competitors can maintain by recognising their mutual interdependence. In a tacitly collusive context, the non-competitive outcome is achieved by each participant deciding its own profit-maximising strategy independently of its competitors. This typically occurs in transparent markets with few market players, where firms can benefit from their collective market power without entering into any explicit communication.[4]

Tacit collusion, also known as oligopolistic price coordination or conscious parallelism, is the agreement that is not considered unlawful by the antitrust authorities worldwide and is generally observed in close concentrated markets where firms set their prices at a profit-maximising, supra-competitive level by recognising their shared economic interests and their interdependence with respect to price and output decisions[5] and under certain conditions, in oligopolistic markets, tacit collusion can lead to a market outcome with

This chapter has been contributed by Drishti Parnami, Fellow, CUTS Institute for Regulation & Competition

higher prices even if there are no explicit or implicit agreements between competitors.

Two essential elements are required for tacit collusion. First, there should be a transparent mechanism for coordinating on a collusive outcome; and second, a plausible amount of mutual understanding among firms.[6]

For tacit coordination to be sustainable over time, several conditions are needed: first of all, it is important that the firms involved in the coordination are able to monitor the activities of all the participants and keep a check that there is no deviation. Second, in case of deviation, a deterrent mechanism can be efficiently activated. Third, the response of other factors outside the coordination should be a concern for the coordinators; that is, present and future competitors not participating in the coordination, and consumers are not able to endanger the results expected from the coordination.[7]

It is noted by a European case, "*there must be an incentive not to depart from the common policy on the market.*"[8]It is recognised by the EU and the U.S. antitrust authorities that tacit collusion is more precarious for the better antitrust enforcement in comparison to the explicit collusion, as for tacit coordination, even when observed, cannot easily be controlled directly by the antitrust laws."[9]

Artificial Intelligence and Tacit Collusion

Tacit collusion has taken another dimension with the proliferation of algorithms. Many competition authorities recognise the risk that algorithms can facilitate and enhance tacit collusion. The OECD in 2016, for example, commented that these "*strategies may pose serious challenges to competition authorities in the future, as it may be very difficult, if not impossible, to prove an intention to coordinate prices, at least using current antitrust tools.*"[10]

The OECD in 2017 reached the following two conclusions: Firstly, "*algorithms are fundamentally affecting market conditions, resulting in high price transparency and high-frequency trading that allows companies to react fast and aggressively.*" These changes in digital markets, if taken to a certain extent, could make collusive strategies stable in virtually any market structure. Second, the companies with advanced algorithms can make their algorithms interact without any direct communication, and the cartel's outcome is achieved through tacit collusion.[11]

Collusion is more easily sustained in oligopolistic markets due to their structural characteristics—few firms, high entry barriers, frequent interactions, and market transparency.[12] These features make it easier for

firms to detect deviations and coordinate to restrict competition. Since each firm's actions significantly affect others, decisions are interdependent, and strategic behaviour often accounts for competitors' likely responses. Conversely, as the number of firms increases, coordination becomes more difficult, incentives for collusion diminish, and potential profits from collusion are divided among more participants.[13]

The growing concentration of electronic retail platforms and the emerging pricing patterns indicate that the online retail industry increasingly resembles an oligopolistic market structure. In such e-commerce environments, the widespread use of similar pricing algorithms and the abundance of market data can push markets that were previously competitive toward tacit interdependence. As a result, instances of parallel pricing may arise not from explicit collusion or intense competition, but from algorithmic tacit collusion.[14]

Major online platforms, therefore, form a narrow oligopoly where technological innovation and market dynamics make coordination easier. The OECD's study on algorithms and collusion highlights those online markets — characterised by high transparency and frequent interactions — are particularly conducive to such behaviour[15]. Algorithms can instantly monitor competitors' actions and process vast amounts of information, significantly reduce coordination costs and enhance the stability of collusive outcomes in digital markets.

Tacit Collusion: Indian Perspective

The preceding section elaborated on the concept of tacit collusion, the market conditions under which it is more likely to occur, and the role of algorithms in facilitating this process. Tacit collusion, as discussed, refers to implicit coordination among market participants, which can be achieved through algorithms without direct human intervention. To examine the jurisprudence surrounding implicit agreements within the Indian context, it is essential to analyse the definition of "agreement" under Indian competition law and the legislative intent behind the term's inclusion in the statute.

Agreement is defined in Section 2 (b) of The Competition Act, 2002, it is defined as any "*arrangement or understanding or action in concert, whether or not formal or in writing or intended to be enforceable by legal proceedings.*

This definition is an inclusive one and covers not only an agreement in the conventional sense under the Indian Contract Act, 1872, but also any arrangement, understanding or action in concert between two or more parties, whether formal or in writing or whether enforceable by law or not. The

definition of agreement has a wide scope; it covers written as well as oral understanding, even a wink or a nod would suffice to fall within the ambit of this definition.[16]

The Government of India constituted a High-Level Committee on Competition Policy and Competition Law, chaired by Mr. S V S Raghavan, in October 1999 to recommend a contemporary, suitable competition legislative framework in line with the new economic policy introduced in 1991 to cope with the international economic developments.

The Raghavan Committee, while discussing the issue of implicit collusion, observed in its report that "*in principle, any kind of agreement (including oral and informal agreements and arrangements) could be illegal, if it violates the law. In the case of written or formal agreements, there can be no legal controversy. On the other hand, in the case of oral or informal agreements, it is necessary to prove the existence of an agreement. Proof will generally be based on circumstantial evidence, and parallelism of action between firms can indicate this. It follows that any prohibitions should also apply to what in the U.K. law are known as "concerted practices". Although the distinction between these and agreements is often imprecise, a concerted practice exists when there is informal cooperation without a formal agreement*".[17]

The Competition Commission of India **in M/s Puja Enterprises & Ors**[18] has interpreted the broader definition of 'agreement'. The CCI was of the view that understanding may be tacit, and the definition covers situations where the parties act on the basis of a nod or a wink. There is rarely direct evidence of action in concert, and the Commission has to determine whether those involved in such dealings had some form of understanding and were acting in co-operation with each other.

In light of the definition of the term 'agreement', the Commission has to find sufficiency of evidence on the basis of the benchmark of 'preponderance of probabilities. In most cases, the existence of an anti-competitive practice or agreement must be inferred from a number of coincidences and indicia which, taken together, may, in the absence of another plausible explanation, constitute evidence of the existence of an agreement. Thus, even an informal co-operation can be construed as an agreement for the purpose of Section 3 of the Competition Act is a meeting of minds.

In the case of Re M/s Sheth & Co,[19] while deciding accusations of collusive bidding, the Commission noted that price parallelism coupled with peculiar market conditions like few enterprises with same owners, stringently standardised product, predictable demand, and other such plus factors point towards collusive tactics adopted by accused enterprises and held their actions to be in violation of Section 3(1) read with Section 3(3) (a) and Section 3(3) (d) of the Competition Act.[20]

From this judgment, it can be inferred that conscious parallelism is not a blanket that will always cover collusion or joint behaviour of the enterprises from legal action and will not clothe culpable enterprises with immunity.[21] The CCI has examined carefully any joint behaviour with the varying facts and circumstances of each case, which could potentially contribute as a plus factor in determining the existence of 'meeting of minds.'

Thus, the CCI relies on the existence of certain 'plus factors' to infer 'meeting of minds' and establish collusion.[22] Plus factors, as defined by the commission, "*are economic actions and outcomes, above and beyond parallel conduct by oligopolistic firms, that are largely inconsistent with unilateral conduct but largely consistent with coordinated action*."[23] The CCI has also held that particular actions of competitors can be construed as evidence of concerted practice where there is no plausible alternative.[24]

However, the approach to determining the adequacy of plus factors in holding parallel behaviours as collusive and not conscious has somewhat been inconsistent. The frequently cited examples to demonstrate the inconsistence are the Cement Manufacturers Case[25] and the Tyre Manufacturers Case.[26]

In Cement Cartel case information was filed by the Builders' Association of India on 26 July 2010 against the Cement Manufacturers association and ACC, Gujarat Ambuja Cements Limited (now Ambuja Cements Limited), Ultratech Cements, Grasim Cements (now merged with Ultratech Cements), JK Cements, India Cements, Madras Cements, Century Textiles & Industries Limited, Binani Cements, Lafarge India and Jaiprakash Associates Limited.

On September 15, 2010, the CCI formed a *prima facie* opinion on the contravention of the Competition Act and directed investigations in the matter. On May 31, 2011, the Director General submitted his report detailing contravention of the Competition Act by the respondents. There were several issues raised in this case pertaining to jurisdiction, failure to cross-examine, and incorrect information in press reports. However, this work focuses on the issue of price parallelism and the oligopolistic structure of the cement market.

On the structure of the cement industry, the CCI observed that no player can be said to be dominant in India. There are 12 major players in the industry, having about 75 percent of the total capacity in India, with about 21 companies controlling about 90 percent market share in terms of capacity. Thus, the cement industry would fall into the category of an oligopoly. In such a market companies tend to note each other moves specifically regarding prices.

The cement companies were held to have violated Section 3 of the Competition Act and were heftily fined. The chief objection taken by the cement companies

was that the DG failed to prove cartels with any direct evidence. Nevertheless, rejecting this contention, CCI noted that cartels are super secretive and also a very serious antitrust offence, therefore in proving such cases circumstantial evidence can be relied on.

Another objection raised by the cement companies was regarding the role of the Cement Manufacturers Association (CMA). It was contented that CMA collects retail and wholesale prices data from different parts of the country and transmits them to the Ministry of Commerce, as per the latter's request. CCI, while rejecting this contention, held that the competitors were interacting using the platform of the CMA and this gave them an opportunity to determine and fix prices.[27]

It was further noted that the association publishes statistics on manufacturing and circulated the detail amongst its members. This information sharing and accessibility makes coordination easy.

In this case, DG has conducted an economic analysis of price data which indicated price parallelism, all the contentions of cement companies regarding inappropriate benchmark of price adopted by CCI, the difference in price as some firms had submitted gross price, others have submitted depot price, average retail price. Apart from price parallelism, there was production parallelism in which production figures have showed a strong correlation. Also, dispatches made by the cement companies have been identical.

Parallel behaviour in prices, dispatch and supply accompanied with some other factors indicating coordinated behaviour among the firms may become a basis for establishing concerted action. Even in foreign jurisdictions, circumstantial evidences have been used and relied upon in cartel cases. Such circumstantial evidences are of no less value than direct evidence as the law makes no distinction between direct and circumstantial evidence.[28] In blatant contrast to this decision, in October 2012, in *All India Tyre Dealers' Federation* case was dealt by CCI. The facts of this case are similar to the cement cartel case discussed above.[29] In this case, information was filed by All India Tyre Federation against tyre manufacturing companies. It was alleged that the domestic tyre industry was indulging in anti-competitive activities and violating Section 3(3)(b) of the Competition Act.

The Commission found that since the tyre manufacturing market is highly concentrated and oligopolistic in nature, in oligopoly markets there are few players thereby each player is aware of the activities of other players. The meetings held by the manufacturers did not amount to cartelisation under Section 3(3) of the Act. It was held that the available evidence did not give enough proof that tyre companies and associations acting together had limited and controlled the production and price of tyres in the market in India. The

CCI found that there was not sufficient evidence to hold a violation by the tyre companies of Section 3(3)(a) and 3(3)(b) read with Section 3(1) of the Competition Act.[30]

It is relevant to note that the Commission had applied the same principles to determine the merits of both cases. There was a visible parallelism in the prices set by the tyre manufactures and the information was exchanged with the help of tyre trade association.[31]

In both cases, active industry trade associations conducted regular meetings. Plant capacities to manufacture the product were much higher than what was being produced by both cement and tyre manufacturers, but they still refrained from cutting costs. In the *Cement case* specifically, the Commission found that in addition to likeness in pricing due to prior consultations between the parties, there was also capacity under-utilisation and production and dispatch parallelism amongst them.[32]

Despite the similar set of facts in both cases, the Commission in Tyre case was of the view that there is no specific patterned behaviour between the parties and the meetings, price parallelism was not sufficient to prove the existence of a cartel.[33]

The OECD report observes that there shall be holistic use of circumstantial evidence, rather than on an item-by-item basis. The information exchange that can facilitate a cartel agreement and its evidence in circumstantial evidence is not enough to prove agreement.[34]

CCI in both the Cement and Tyre cases had cited this OECD report, but seems to apply its recommendations selectively as it has failed to set a uniform threshold to establish cartelisation. In a cartel case, communication plays a very important evidence; it is the evidence that cartel operators met or otherwise communicated. However, in oligopolistic markets, providing pricing information to a third-party trade association is often inadequate circumstantial evidence.

Yet, in the *Cement case,* the Commission found that examples of such communication were sufficient, in spite of signs explaining that the conduct of Cement manufacturers was consistent with their self-interests. Moreover, the oligopolistic market type and similarity in demand and pricing of almost identical products was seen as a sufficient justification in the *Tyre case*, but discarded in the *Cement case.*

In a more recent case of Rajasthan Cylinders and Containers Limited vs Union of India and another,[35] the CCI had ruled that suppliers of Liquefied

Petroleum Gas (LPG) Cylinders to the Indian Oil Corporation Ltd had been involved in cartelisation, thereby influencing and rigging the prices, and subsequently, violating the provisions of Section 3(3)(d) of the Competition Act. This decision was upheld by COMPAT.

However, the Supreme Court rejected the decision of both CCI and COMPAT. It established that there might not be direct evidence to prove cartelisation or anti-competitive practices; in such situations, circumstantial evidence can be relied on. Parallel or similar prices can prove to be strong evidence of collusion. But when it comes to oligopoly markets, it cannot be considered conclusive. Some more evidence needs to be taken into account before determining an anti-competitive agreement.[36]

Supreme Court viewed that CCI's conclusions were based on the plus factors, including but not limited to market conditions, presence of a number of players, and submission of identical bids (with varying costs) that it had taken into account[37] and that these factors were "only one side of the coin"[38] and had to be evaluated by keeping the ground realities in place. Both the COMPAT and, subsequently, the Supreme Court accepted the theory of oligopolistic interdependence[39] and held the parallel conduct to be a consequence of the structure of the market.

From the cases discussed above, it can be concluded that notwithstanding the broad language of Section 2 and 3(3) of the Competition Act which is capable of taking a wide range of anti-competitive conduct within its ambit, the inconsistency with respect to the acceptability of evidence in order to establish plus factors, and the differences in understanding the nature of oligopolistic markets somewhat messes the true practicable scope of the provision.

In recent rulings by the Supreme Court of India, it has become evident that courts are seeking evidence beyond mere parallel pricing to establish the existence of cartels. They emphasise the need for additional "plus factors" as corroborative evidence. Cartel cases are inherently complex and carry significant penalties, necessitating a careful approach to ensure that innocent parties are not wrongfully penalised.

Two contrasting approaches have emerged in such cases. On one hand, the CCI has, in certain instances, imposed penalties based on evidence such as uniform pricing, communications through trade associations, underutilisation of production capacity, and similar indicators. On the other hand, in other cases, both the CCI and the Supreme Court have deemed such factors insufficient and have emphasised the requirement of additional "plus factors" to conclusively establish a cartel.

The next segment focuses on the concept of "plus factors" in cartel investigations, analysing what constitutes such evidence and identifying specific actions and behaviours that may be categorised as "plus factors" to substantiate cartel allegations.

Plus Factors

"*Plus factors are economic actions and outcomes, above and beyond parallel conduct by oligopolistic firms that are largely inconsistent with unilateral conduct but largely consistent with coordinated action.*"[40]

While delving into the 'parallelism plus factors', the CCI has also time and again adopted the '*but for'* test. This test is applied to determine whether the conduct of the parties' firms in the nature of parallel behaviour would have taken place "*but for the agreement, decision or practices of the enterprises*[41]".

Plus factors are small pieces of evidence that can be used to strengthen the case of cartelisation. They include a small number of firms in the market, high barriers to entry, relatively inelastic demand and so on. As cartels are a serious offence and it can cause serious damage to the whole industry and economy of a nation, it is necessary to handle the case with utmost care and vigilance. Parallelism plus can be considered as the evidentiary standard required to prove a cartel. The evidence must be sufficient to "*exclude every possibility but the one proposed to be proved*" or "*to show that within all human possibility, the respondents must have acted in concert.*"[42]

With plus factors in place, competition enforcement authority does not have to prove the existence of an agreement but has to prove that in light of various economic indicia, concerted action is the most plausible explanation for the parallelism in prices.[43]

The competition authority has to show that price parallelism exists, along with a number of plus factors that strengthen the suspicion of the court that the firms were acting in concert.

Plus factors can include the evidence of regular communication between firms, industry performance data that will include low supply, and resources that are not used in an optimum manner can be taken as evidence.[44]

Plus factors found as sufficient to conclude that there was a collusion when the fact that: (i) the first company to raise the price was the company with the lowest market share; (ii) there wasn't an increase in costs that could explain the joint increase of prices; and (iii) the companies used the same way at almost the same time to communicate the price raising or the joint meeting.[45]

In the *LPG cylinder manufacturer*'s case discussed above, it was observed that the plus factors used to determine the existence of cartel plus factors can include a small number of suppliers, few new entrants, an active trade association, repetitive bidding, homogenous products, few or no substitutes and lack of significant technological changes. In India, since the inception of the Competition Act, it is established that in an oligopolistic industry, the firms recognise their mutual interdependence, acknowledge that they are players in a repeated game, and act according to it. In antitrust decisions, mere conscious parallelism does not suffice for the determination of firms engaged in concerted action because such pricing can emerge from firms acting non-collusively where they understand their role as players. In such cases, it is required that economic circumstantial evidence go beyond the parallel movement in price to reach a finding that the firms have crossed that line, thereby violating the provisions of the Act.[46]

In Film & Television Producers Guild of India v. Multiplex Association of India,[47] it was held that trade associations could be used as platforms for the exchange of information by competitors in order to conduct concerted activities; however, the mere fact that meetings were conducted for sharing information cannot result in anti-competitive consequences.

Conclusion and Recommendations

Cartels can be identified and sanctioned even in the absence of direct evidence of an agreement. Key questions in the present context are: how does algorithm-driven collusion differ from traditional forms of collusion that authorities have long addressed, and whether algorithm-driven tacit collusion can be classified as *per se* anti-competitive?? This accelerated dynamic implies that in digital markets with oligopolistic structures, the likelihood of parallel behaviour emerging is significantly higher and occurs much sooner than in traditional markets, even under similar conditions.

In such virtual environments, after a certain threshold of interactions, competitors may find it economically optimal to coordinate their behaviour, maintaining supra-competitive prices rather than competitive ones. This dynamic poses substantial risks to consumer welfare and economic efficiency, underscoring the need for a re-evaluation of antitrust frameworks to address the unique challenges posed by algorithm-driven tacit collusion.[48]

The advent of algorithms has elevated the clandestine nature of pre-existing tacit collusion. Hence, the challenge is now for the Competition regulators to carefully employ competition assessment tools while addressing this rather new AI-driven collusion. In this regard, the suggestions of Professor Ezrachi could prove to be useful.[49]

For instance, he suggested that agencies to audit algorithms, where the Competition Regulators will assess whether the algorithm can oil the wheels of collaborative outcomes or price alignments. Algorithmic auditing ranges from regulatory inspection to determine whether an algorithm is compliant with a law, regulation or norm, where regulators or auditing professionals can use a variety of tools or methods.[50]

Implementing such a mechanism would require advanced technical expertise and substantial resources. Moreover, issues like commercial confidentiality and the inherent complexity of auditing self-learning algorithms render this solution less feasible. Self-learning algorithms, while potentially pricing competitively within the controlled environment of a sandbox, could develop novel strategies through repeated real-world interactions, thereby undermining the effectiveness of pre-deployment evaluations.

Another feasible way to assess the anti-competitive nature of an algorithm is to use an algorithm collusion incubator, whereby a self-developed algorithm is used by the competition regulator to imitate the results that are observable in the market and based on that try to assess what actually led to a series of instructions that resulted in anti-competitive conduct. Other possible countermeasures included: 1) de-acceleration, or semi-deceleration, where algorithms are restricted from instantaneously adjusting prices to competitors' prices; 2) disruptive or consumer algorithms; and 3) sponsored entry to destabilise the algorithmic collusive market.

As there has been no unified approach in dealing with tacit collusion, and the plus factors will vary according to the case, it has amounted to conflicting opinions about the issue as discussed above in the cement, steel and LPG cylinder case. Definitely, for determining the existence of tacit collusion, economic factors have to be considered. In this regard, the first step CCI has taken is to establish a digital market unit. The Division has a core team of seven, with training focused on AI, data analytics, and algorithmic modelling.

In India, one of the notable cases that sheds light on the crossroads of competition law and AI is Samir Agarwal v. ANI.[51] In its pith and substance, it was alleged by the Petitioners that "Ola" and "Uber" were in the position of a "hub" for their respective drivers' "spokes" which resulted in collusion. Further, it was contended that Ola and Uber were fixing prices between their drivers through the use of their separate algorithms, thereby triggering the provision of Section 3 of the Competition Act 2002.

However, the Supreme Court categorically held that there was no hub and spoke model in the current case as neither Ola nor Uber were aware of each other's prices and both the entities acted in the capacity of principals for their respective drivers, thereby ruling out the contention of a hub. The fact

that drivers held the autonomy to accept and reject rides showcased the lack of control the enterprises had on them.

The recently released CCI's Market Study on AI[52] can act as a stepping stone in the journey of AI regulations. The study suggests a self-audit of AI systems for competition compliance, where the CCI has also provided a draft template for self-check starting from design, testing, monitoring, transparency and integration. Further, the study suggests that business players to adopt a transparent and lucid way of integrating AI, where each step of the algorithm is explainable without jeopardising the proprietary data of the customers.

Additionally, the study also suggests for a time-to-time advocacy workshop conducted by the CCI to keep up with the pace of rapidly changing developments made in this industry. The report also provides measures to lower entry barriers, including improved access to data and national AI computing infrastructure and promotion of open-source frameworks.

In the end, the study is applauded for its recognition and emphasis on international cooperation with authorities like OECD, ICN, UNCTAD. Hence, while AI has become the new normal in business practices, CCI's Market Study has formally opened the doors for discussion on the crossroads of AI and competition law. A lot of measures are yet to be taken on incorporating a framework that protects market competition without acting as a hindrance in AI advancements.

Further, to mention the note by European Competition Commissioner Margrethe Vestager. She referred to the risk that algorithms pose as serious; however, this does not mean that competition enforcers should be suspicious of everyone who uses any algorithm. Competition enforcers must be vigilant and able to deal with the competition challenges posed by algorithms. She recommended a "*compliance by design*" approach, which means that businesses that are developing algorithms should design them in a manner that doesn't allow them to collude, and the firms also need to know that when they decide to use an automated system, they will be held responsible for what it does.[53]

Therefore, it is suggested that the firms should refrain from using algorithms that may facilitate tacit collusion, even if their usage has a legitimate justification.

Endnotes

1 *Brooke Grp. v. Brown & Williamson Tobacco Corp.*, 509 U.S. 209,227, 113 S. Ct. 2578 (1993)

2 *Monsanto Co. v. Spray-Rite Serv. Corp.*, 465 U.S. 752,765 104 S. Ct. 1464 (1984), at 624

3 Louis Kaplow, *Competition Policy and Price Fixing* (Princeton University Press, 2013) 8.

4 *Supra note* 2

5 *Supra note* 1

6 OECD (2023), Algorithmic Competition, OECD Competition Policy Roundtable Background

7 Ariel Ezrachi, Maurice E. Stucke, *'Tacit Collusion on Steriods - The Tale on Online Price Transparency, Advanced Monitoring and Collusion'*, (3 CLPD 24 2017).

8 *Airtours plc v. Commission of European Communities* [2002] ECR-II-2585

9 *F.T.C. v. H.J. Heinz Co.*, 246 F.3d 708 (D.C. Cir. 2001)

10 OECD, *'Big Data: Bringing Competition Policy to the digital era'*, (Oct 27, 2016), <https://www.oecd.org/competition/big-data-bringing-competition-policy-to-the-digital-era.htm>

11 *Supra note* 5.

12 Ivaldi, Jullien, Rey, Seabright, Tirole, *'The Economics of Tacit Collusion'* (March 2003), <https://www.bateswhite.com/assets/htmldocuments/media.730.pdf>

13 Carl Shapiro, Theories of Oligopoly Behaviour, in R. Schmalensee & R.D. Willig (eds), HANDBOOK OF INDUSTRIAL ORGANIZATION 329 (.,1st ed. 1989).

14 Reinhard Selten, 'A Simple Model of Imperfect Competition, Where Four Are Few and Six Are Many', (1973) 2 INT'L J. GAME THEORY 141

15 J. Mordall, 'OECD Workshop Addresses Algorithms and Collusion Issues', (Kluwer Competition Law Blog,17 July 2017), <https://competitionlawblog.kluwercompetitionlaw.com/2017/07/17/oecd-workshop-addresses-algorithms-collusion-issues/> accessed 19th November 2024

16 Competition Commission of India, *'Introduction to the basics of competition law'*, (Aug, 2016), <https://www.cci.gov.in/sites/default/files/advocacy_booklet_document/CCI percent20Basic percent20Introduction_0.pdf>

17 Indian Competition Law Review, <https://theindiancompetitionlaw.files.wordpress.com/2013/02/report_of_high_level_committee_on_competition_policy_law_svs_raghavan_committee.pdf >accessed June 26, 2021

18 **Case No.1 of 2012**

19 CCI, Suo Motu Case No. 04 of 2013, *In Re: M/s Sheth and Co, and Others*, Suo Motu Case No. 04 of 2013.

20 *Suo Motu* Case No. 04 of 2013, 38.

21 *Theatre Enterprises Inc. v. Paramount Film Distributing Corp*, 346 U.S. 537 (1954).

22 *All India Tires Dealers Federation v. Tire Manufacturers,* MRTP Case: RTPE No. 20 of 2008.

23 *MRTP Case*: RTPE No. 9 of 2008,123.

24 *MRTP Case:* RTPE No. 20 of 2008.

25 *Builders Association of India v. Cement Manufacturers' Association.,* Case No. 29 of 2010

26 *Supra Note 24*

27 *Supra Note 25*

28 *Supra Note 25*

29 Umakant Varotill, 'Summary of CCI order against cement companies', (2012) INDIAN CORP LAW <https://indiacorplaw.in/2012/06/summary-of-ccis-order-against-cemen.html> accessed 20th November 2024

30 Section 3(3)(a) and 3(3)(b), read with Section 3(1) of the *Competition Act, 2002*, prohibit agreements between enterprises or associations of enterprises that have an appreciable adverse effect on competition (AAEC) within India. Specifically, Section 3(3)(a) proscribes agreements that directly or indirectly determine purchase or sale prices, while Section 3(3)(b) forbids agreements that limit or control production, supply, markets, technical development, investment, or provision of services. When read with Section 3(1), these provisions collectively establish a presumption of anti-competitive intent for such horizontal agreements, including cartels, unless proven otherwise.

31 Harshvardhan Korada, 'CCI Imposes Penalty of INR 17.88 Billion On Five Tyre Manufacturers For Cartelisation', (Mondaq, 16 February , 2022), https://www.mondaq.com/india/cartels-monopolies/1161796/cci-imposes-penalty-of-inr-1788-billion-on-five-tyre-manufacturers-for-cartelisation

32 *Supra note* 143, para 365.

33 Priya Urs, Rishi Shroff, 'The Cement and Tyre Cartels: What India Can Learn from the US and EU', INDIAN LAW JOURNAL, <https://www.indialawjournal.org/archives/volume6/issue-2/article4.html>accessed 21st November 2024

34 OECD, Prosecuting Cartels without direct evidence, DAF/COMP/GF (2006) 7, (Sept 11, 2006), https://www.oecd.org/daf/competition/prosecutionandlawenforcement/37391162.pdf

35 *Rajasthan Cylinders and Containers Limited v. Union of India and another*, Civil Appeal No. 3546 of 2014.

36 Shivani Chauhan, 'Case Study: Rajasthan Cylinders and Containers Limited v. Union of India and another', (Aug 3, 2020), <https://legal-wires.com/case-study/case-study-rajasthan-cylinders-and-containers-limited-v-union-of-india/>accessed 21St November 2024

37 *Supra Note 35*

38 *Ibid* at 88.

39 Richard Whish, David Bailey, '*Competition Law*', 10th ed. (Oxford University Press, 2018).

40 *In Re: Alleged cartelization by steel producers*, Case No.: RTPE No. 09 of 2008 (MRTP)

41 Shubha Ojha, 'Carving out the evidentiary standards under section 3(3) via CCI's decisional practice', (I Pleaders, (March 30, 2021), https://blog.ipleaders.in/carving-evidentiary-standards-section-33-via-ccis-decisional-practice/

42 *Hanuman v State of Madhya Pradesh*, AIR 1952 SC 343.

43 *Builders Association of India v Cement Manufacturer's Association*, Case No. 09/2010.

44 Andrew I. Gavil Et Al., '*Antitrust Law in Perspective: Cases, concepts and problems in competition policy',* 267-68 (2d ed. 2008).

45 CUTS International, National Law University, Jodhpur, 'Study of Cartel Case Laws in Select Jurisdictions – Learnings for the Competition Commission of India', (April 25, 2008), <https://www.cci.gov.in/images/marketstudie/en/docs1652440423.pdf>

46 *In Re: Alleged cartelization by steel producers*, Case No.: RTPE No. 09 of 2008 (MRTP)

47 Case No. 37/2011

48 OECD, 'Competition Enforcement in Oligopolistic Markets', DAF/COMP/M(2015)1/ANN10/FINAL, (March 19, 2016), <https://one.oecd.org/document/DAF/COMP/M(2015)1/ANN10/FINAL/en/pdf>

49 OECD, Summary of Discussion of the Roundtable on Algorithms and Collusion, Annex to the Summary Record of the 127th Meeting of the Competition Committee, June 21-23, 2017 (DAF/COMP/M (2017)1/ANN2/FINAL, September 26, 2018)

50 Supra note 6

51 APS Law, 'Case Summary: Samir Agrawal v Competition Commission of India (2020) | Anti-Competitive Agreements' (APS Law, December 15, 2020)

52 Competition Commission of India, 'Market Studies and Research – Competition Commission of India launches market study on Artificial Intelligence and competition' (Press Release, 9 September 2024)

53 Joint study of the French Autorité de la concurrence and the German Bundeskartellamt, 'Competition law and big data', (May 10, 2016), <https://www.autoritedelaconcurrence.fr/sites/default/files/2021-11/big_data_papier.pdf>accessed 22 November 2024

CHAPTER 5

The Copyright Conundrum of Generative AI Training: An Indian Legal Analysis

Introduction

The advent of Artificial Intelligence (AI) marks a watershed moment, reshaping industries, artistic expression, and knowledge dissemination. This cathartic shift, however, casts a long shadow over established intellectual property frameworks, particularly copyright law. In India, a nation rapidly embracing technological advancements while cherishing its rich cultural heritage, the interplay between AI and copyright presents a unique set of challenges and opportunities.

Unlike rule-based tools that confined themselves to mechanistic reproduction, contemporary GenAI models leverage deep learning architectures to generate text, images, audio, and video that closely mimic, and at times rival, human expression. This capacity has broadened the creative and commercial horizons of industries ranging from media and entertainment to education and healthcare, thereby raising significant questions regarding how law ought to engage with technologies that simultaneously promise innovation while testing long-settled normative boundaries.

Intellectual property law and copyright, in particular, sit at the heart of these questions. The core of the legal dilemma lies in the nature of GenAI training. Models are trained on colossal datasets, often scraped from publicly available sources, which invariably include a vast amount of copyrighted content. This process is not a simple act of copying. Instead, the AI system ingests the data, identifies latent patterns, structures, and statistical relationships, and then uses this abstract knowledge to generate new content.

The output, while statistically original, is fundamentally derivative in a non-traditional sense, as it is born from the "computational abstraction" of pre-existing works. The legal tension is clear: does this non-human, large-

This chapter has been contributed by Jameela Sahiba, Associate Director- AI and Public Affairs, The Dialogue

scale ingestion of copyrighted material for the purpose of pattern recognition constitute an infringement? Or is it a transformative use that should be permissible under law, similar to how a human artist learns from studying countless works of art?

This paper explores the copyright-related implications of GenAI within the limited, but critically significant, context of the training phase. By deliberately excluding questions related to authorship, ownership, and liability in the output stage, the paper maintains a focused inquiry into how existing copyright doctrines apply, or fail to apply, to the ingestion and utilisation of copyrighted data by GenAI systems. The training process is foundational to the architecture of GenAI and thus raises threshold legal questions that cannot be resolved by simply deferring to end-use or output-based analysis.

In the Indian legal context, the inquiry is situated against the framework of the Indian Copyright Act, 1957,[1] a statute whose core provisions were conceived in a pre-AI era and are yet to be substantively updated to address the challenges of machine learning systems. While the Act recognises concepts such as fair dealing, temporary storage, and use for research, these provisions were not drafted with algorithmic consumption in mind. Whether the non-human, large-scale, and often non-consensual use of creative works for training GenAI systems can be reconciled with the existing statutory exceptions is a question that remains legally unresolved and doctrinally underdeveloped.

Understanding GenAI's Learning Paradigm

To grasp the copyright implications of GenAI's input stage, it is essential to visualize its operational mechanism through an analogous human learning process. Consider how a child acquires literacy and language: initially, through copying, imitating, and repetitive tracing of alphabets, followed by the progressive mastery of words, sentences, and complex linguistic structures. Similarly, speech development involves constant listening and repetition of sounds and words from caregivers. This foundational exposure intrinsically shapes the child's cognitive architecture, enabling him to not only be influenced by, but also contribute to, the cultural realm.

GenAI systems precisely mimic this "being shaped by, and at the same time shaping back, the cultural realm" through their sophisticated algorithms. These algorithms "read" immense digital datasets, referred to as 'training sets,' to extract 'knowledge.' This knowledge is not a mere reproduction of the original content but rather the meta-information embedded within it. The process involves three fundamental steps[2]:

(1) tokenisation, where data is broken down into fundamental units;
(2) statistical pattern identification, where the system learns the relevance and context of tokens by analysing their placement; and
(3) predictive application, where this learned statistical knowledge is used to generate "reasonable continuations" of text or other media.

Essentially, GenAI converts words and other data into numerical representations (tokens) and identifies massive statistical patterns, mirroring the learning and knowledge-sharing process of a human mind. Far from simply copying, creators of GenAI tools are, in essence, attempting to construct a digital "brain" that learns in a manner conceptually similar to natural human cognitive development.

The Nuance of "Copying" and "Storage" in GenAI Training

The training of GenAI models inherently involves making copies (fixing) of datasets, which often include copyright-protected works, and storing them for varying durations. The critical distinction here, from a copyright perspective, lies in the *purpose* and *exposure* of these copies. Unlike traditional acts of reproduction, where the intent is often to expose or consume the expressive form of the work, GenAI models utilise these copies solely for extracting meta-information.

This meta-information, consisting of statistical patterns and relationships, is then used to "weigh the model and parameters" to gauge the logic of the next possible sequence of tokens. The content itself is not "read" or "enjoyed" by a human in the traditional sense of consuming a copyrighted work for its expressive purpose. For instance, a musician's primary purpose in composing a song is entertainment, not its use for AI training.

The act of "copying" and "storing" are distinct legal acts under the Indian Copyright Act. Section 14(a)(i)[3] of the Act explicitly grants copyright owners of literary, dramatic, and musical works the exclusive right to "reproduce the work in any material form, including the storing of it in any medium by electronic means."

Similar provisions exist for artistic works (Section 14(c)(i)), cinematographic films (Section 14(1)(d)(i)), and sound recordings (Section 14(1)(e)(i)). While the Act does not define "reproduction" or "copy," Section 2(m)[4]'s definition of an "infringing copy" suggests a distinction between "reproduction" and "making a copy" for different work types, arguably emphasising the reproduction of *expressive forms* over mere physical copying. The Delhi High Court in *MRF v. Metro Tyres* (2019)[5] has indeed interpreted "copy" expansively to include imitation of substance, not merely physical replication.

The inclusion of "storing" within the reproduction right by the 1994 Amendment,[6] primarily to align with TRIPs obligations concerning broadcasters and phonogram producers and clarified by the 2010 Parliamentary Standing Committee Report,[7] was primarily aimed at preventing unauthorised exposure of content by Internet Service Providers. This historical context is crucial: the focus was on preventing economic harm in the *primary market* by substituting the original work's expressive form or unauthorisedly exposing its originality.

The Idea-Expression Dichotomy and Transformative Use in Training

The cornerstone of copyright law, the idea-expression dichotomy, explicitly limits protection to the expressive form of a work, not the underlying ideas or information. Article 9.2 of the TRIPs Agreement[8] reinforces this, stating that copyright protection extends only to the "original way" in which information or ideas are expressed.

The Supreme Court of India, in *R.G. Anand v. Delux Films* (1978),[9] emphasised that infringement occurs when the "manner, arrangement, situation to situation, scene to scene with minor changes or super additions have been adopted," as opposed to merely appropriating the underlying idea or information.

The Calcutta High Court, in *Barbara Taylor Bradford v. Sahara Media* (2003),[10] further underscored that only the appropriation of expression, not ideas, constitutes infringement. This rationale stems from the fundamental principle that copyright incentivises the creation of *concrete forms* of expression, not the monopolisation of information or facts themselves. The Delhi High Court, in *Wiley Eastern Ltd. v. Indian Institute of Management* (1995),[11] has also recognised copyright's conscious restriction to avoid stifling free speech under Article 19(1)(a) of the Indian Constitution.

This perspective is bolstered by doctrines like merger doctrine[12] (where ideas can only be expressed in a limited number of ways or are functional/genre-specific) and the de minimis rule[13] (where trivial parts of a work are used without constituting a substantial part of the expressive form). These doctrines collectively underscore that the reproduction right primarily protects against the unauthorised *exposure* or *consumption* of the expressive forms of a work, ensuring creators are recompensed in their primary markets. They do not aim to stifle the flow of ideas or extract meta-information from these expressions.

The pivotal question for Indian courts, therefore, becomes: Does copying or storing copyrighted material for GenAI training, which is entirely non-expressive and non-consumptive (i.e., not exposing the expression to any

human but solely extracting meta-information for model weighting and parameter training), constitute copyright infringement?

This is akin to asking whether using a copyrighted book as a doorknob (as an example cited by scholars) infringes copyright merely because a physical copy was made, or whether plagiarism software storing student papers to detect similarities (*A.V. v. Iparadigms, Limited Liability Company*, 2008[14]), or web-crawling software making cached copies for search engine functionality (*Field v. Google*, 2006[15]), or even Google Books creating searchable indices (*Authors Guild v. Google*, 2015[16]), constitute infringement of the reproduction right.

A purposive interpretation of "reproduction, including storing of works" under Section 14[17] of the Act, would likely exclude an exclusive right over storage that is not for expressive reproduction but solely for meta-information extraction. This aligns with the idea-expression dichotomy, where the physical fact of storage or copying becomes irrelevant as long as the protected expressive form is not exposed or exploited in a manner that substitutes the original market. Conversely, a literal construction could lead to an expansive interpretation, extending the primary market of the copyright owner to mere storage or copying, irrespective of its expressive context. The judicial trajectory in India will critically determine this outcome.

Transient Storage and Incidental Use

Even if storage for GenAI training were deemed infringing under a literal interpretation of Section 14, specific exemptions under Section 52(1)(b) and (c)[18] of the Act regarding transient or incidental storage offers potential legal pathways for AI developers. These provisions exempt transient or incidental storage occurring purely in the technical process of electronic transmission or for providing electronic links or access, provided it is not expressly prohibited or infringing.

The core questions for courts to grapple with are: (a) whether the storage of training datasets for the model training period can be considered "transient"; and (b) whether such storage would be deemed "incidental" to the primary function of providing access to the GenAI model for meta-information extraction.

The Delhi High Court's ruling in *MySpace Inc. v. Super Cassettes Industries Ltd* (2016)[19] provides some interpretive guidance. The court held "transient" to mean temporary and "incidental" to mean subordinate to a greater, permissible function. This was applied to "cached data" and other data generated automatically to improve the performance of a core, permissible function.

Crucially, the legislative intent behind Section 52(1)(c)[20] indicates that storage is permissible when the resulting exposure is non-infringing.

Therefore, a compelling argument can be made that storage solely for the functionality of training, which is arguably a transformative and permissible purpose of meta-information extraction, constitutes "incidental storage" permissible under Section 52.[21]

Further, the "transient" nature of storage would depend on its duration; if data is automatically removed once its meta-information is extracted and absorbed by the model, especially without human exposure, it could arguably fall within this exception. This interpretation supports an environment where AI models can learn and evolve without undue legal encumbrances, fostering innovation in line with global advancements. However, judicial clarification will be essential to solidify these interpretations within the Indian legal landscape.

The Contours of the Debate: AI, Copyright, and the Path Forward

The evolving discourse around genAI and copyright in India is not merely a legal question of statutory interpretation, it is, at its core, a normative conversation about the future of creativity, technological sovereignty, and economic growth. As policymakers, scholars, and industry stakeholders grapple with the implications of AI training practices, a consensus is emerging around a singular reality: the existing copyright framework, while foundational, is increasingly ill-equipped to deal with the scale, complexity, and technical nature of machine learning processes.

The challenge, therefore, is not whether the law must evolve, but how it should evolve in a manner that preserves the essential incentives of copyright while enabling India to remain competitive in an AI-driven global economy.

Competing Conceptions of Copyright in the AI Era

At the heart of the debate lie two competing conceptions of copyright's role in the age of AI. The first, often championed by authors' rights groups and collecting societies, holds that any unlicensed ingestion of copyrighted works, regardless of its purpose or expressive outcome, constitutes a violation of the reproduction right. From this perspective, the fact that AI models copy and store entire works during training is dispositive; the absence of human consumption or expressive reproduction does not absolve the act of its infringing character. This view places a premium on strong proprietary control, arguing that it is only through robust enforcement that creative industries can sustain themselves in the face of rapid automation and disintermediation.

The second conception, advanced by technologists, economists, and increasingly by a cohort of legal scholars, urges a more functionalist interpretation of copyright in the context of AI. Here, the focus shifts from the mere physical act of copying to the purpose, nature, and market effect of that use.

Training a model, in this view, is fundamentally distinct from expressive reproduction: it is a non-substitutive, non-exploitative act aimed at extracting patterns and correlations, rather than communicating a work to the public. To conflate such computational analysis with infringement, proponents argue, is to risk weaponising copyright law against the very innovation it was designed to stimulate.

What Could Be a Pragmatic Middle Ground?

On the one side, industry representatives and AI developers have emphasised the chilling effect that legal uncertainty exerts on innovation. They argue that the absence of explicit exceptions or clarifications around the training process disincentivises investment, discourages domestic startups, and risks ceding technological leadership to jurisdictions with more permissive legal regimes.

On the other, rights holders have cautioned against diluting the exclusive rights enshrined in the Copyright Act, warning that unchecked algorithmic use could undermine licensing markets and erode creators' economic incentives. Between these poles, the Indian exploration of finding a middle path continues; one that neither grants carte blanche to developers nor imposes prohibitive constraints on innovation. Central to this emerging consensus is the potential utility of a text and data mining (TDM) exception, carefully tailored to India's socio-economic context and technological ambitions.

Text and Data Mining

The appeal of a TDM-oriented approach lies in its ability to reconcile the core concerns of both camps. Properly crafted, a TDM exception can preserve the economic interests of rights holders, for instance, by limiting its scope to non-expressive uses, imposing transparency obligations, or providing opt-out mechanisms for sensitive works, while simultaneously providing the legal certainty necessary for AI research and commercial deployment.

Such a provision would not be without precedent. Jurisdictions as diverse as Japan[22, 23, 24] Singapore, and the European Union[25] have enacted TDM exceptions, recognising that the mere act of computational analysis does not meaningfully interfere with the market for the original works. India, with its rapidly expanding digital economy and burgeoning AI sector, arguably has even stronger reasons to adopt a similar approach. Doing so would align

its legal framework with global best practices, reduce compliance costs for innovators, and bolster its strategic positioning as a hub for AI development.

The Limits of Alternative Approaches

Alternative policy mechanisms, such as mandatory licensing regimes or remuneration schemes, have also been proposed as potential solutions. Yet, they present significant doctrinal and practical challenges. A compulsory licensing system, while theoretically ensuring compensation, risks imposing disproportionate burdens on nascent enterprises and academic research institutions, which may lack the resources to negotiate or pay for access to vast datasets. Moreover, such systems often fail to reflect the non-expressive, non-substitutive nature of AI training, treating it instead as a form of downstream exploitation.

Similarly, remuneration-based models, which envisage collective management organisations distributing fees derived from AI training, risk entrenching market incumbents and creating inefficiencies. They also offer little legal certainty, as they typically rely on voluntary participation or negotiated settlements rather than statutory clarity. Compulsory Licensing Regimes have also been proposed as a compromise solution. By mandating licensing frameworks for training data, creators would be compensated, and AI actors would gain legal certainty.

Yet, the administrative burden of licensing millions of disparate works renders this option impractical at scale. The complexity of monitoring compliance and calculating royalties also risks ossifying the innovation environment. Further, Sui Generis Rights in Data have also periodically been suggested, creating a new form of protection for information used in AI training. However, extending property rights into the realm of non-expressive data risks over-enclosure, stifling creativity by restricting access to information that has never before been proprietary. In contrast, a narrowly defined TDM exception provides an *ex ante* legal framework that is both more predictable and more innovation friendly.

Charting the Way Forward

For India, the path ahead lies in a deliberate recalibration of its copyright regime, one that is responsive to the realities of algorithmic creativity while faithful to the constitutional mandate of promoting the progress of science and useful arts. This recalibration need not amount to a wholesale abandonment of copyright's protective function. It is unlikely to lie in wholesale transplantation of foreign approaches as well, nor in blind adherence to older doctrinal formulations. Instead, what is required is a context-sensitive

framework that prioritises certainty and proportionality. Any such approach needs to signal clarity on three points.

First, that training for machine learning, when limited to the extraction of latent patterns from lawfully accessible sources, ought to be treated differently from unauthorised expressive reproduction. Second, that safeguards may be introduced to ensure accountability at the output stage, thereby preventing substitutive or exploitative uses of copyrighted works. Third, that adopting a tailored statutory clarification, potentially modeled on a TDM-style exception, could provide innovators with the certainty they require while ensuring India's aspiration toward technology-driven growth remains on course.

Conclusion

India's journey in integrating AI with its copyright framework will be a dynamic process. The existing legal structures provide a foundation, but the speed and scale of AI innovation necessitate careful adaptation. The proactive engagement of the Indian government through initiatives like the DPIIT multi-stakeholder committee[26], coupled with the responsible practices emerging from the AI industry, indicate a strong commitment to finding constructive solutions.

A balanced and progressive approach for India must:

a. Foster a collaborative ecosystem: Encourage open dialogue and partnership between AI developers, content creators, legal experts, and policymakers to co-create sustainable frameworks.

b. Ensure legal certainty for AI training: Provide clearer guidelines or specific provisions for text and data mining, promoting innovation while respecting intellectual property.

c. Leverage technological solutions: Encourage the AI industry to lead in developing and deploying advanced technical tools to detect and mitigate potential copyright infringement within AI outputs.

By pursuing these principles, India can effectively harness the groundbreaking power of AI, leveraging the ingenuity of its technology sector, while simultaneously safeguarding the vibrant creative industries that enrich its cultural tapestry. This balanced approach will ensure that AI serves as a powerful engine for progress, responsibly and equitably.

Endnotes

1 The Copyright Act 1957 https://copyright.gov.in/documents/copyrightrules1957.pdf

2 Sneha J and Akshat A, *Indian Copyright Law and Generative AI* https://www.saikrishnaassociates.com/indian-copyright-law-and-generative-ai/

3 Section 14, The Copyright Act, 1957 https://www.copyright.gov.in/Documents/Copyrightrules1957.pdf

4 Section 2, The Copyright Act, 1957 https://www.copyright.gov.in/Documents/Copyrightrules1957.pdf

5 MRF Limited. vs Metro Tyres Limited (2019) https://indiankanoon.org/doc/78110318/

6 Copyright (Amendment) Act, 1994 https://copyright.gov.in/Documents/Notification/Copyright_Amendment_1994.pdf

7 Report on the Copyright (Amendment), 2010 https://copyright.lawmatters.in/2010/11/report-of-psc-on-copyright-amendment.html

8 https://www.wto.org/english/res_e/publications_e/ai17_e/trips_art9_jur.pdf

9 *R.G. Anand v. Delux Films* (1978) https://indiankanoon.org/doc/1734007/

10 *Barbara Taylor Bradford v. Sahara Media* (2003) https://indiankanoon.org/doc/757852/

11 *Wiley Eastern Ltd. v. Indian Institute of Management* (1995) https://indiankanoon.org/doc/1017103/

12 https://www.theipmatters.com/post/the-merger-doctrine

13 https://www.ipandlegalfilings.com/de-minimis-copyright-infringement-where-to-draw-the-line/

14 *A.V. v. Iparadigms, Limited Liability Company*, 2008 https://www.internetlibrary.com/cases/lib_case577.cfm

15 *Field v. Google*, 2006 https://scholar.smu.edu/cgi/viewcontent.cgi?article=1081&context=scitech

16 *Authors Guild v. Google*, 2015 https://www.copyright.gov/fair-use/summaries/authorsguild-google-2dcir2015.pdf

17 Section 14, The Copyright Act, 1957 https://www.copyright.gov.in/Documents/Copyrightrules1957.pdf

18 Section 52, The Copyright Act, 1957 https://www.copyright.gov.in/Documents/Copyrightrules1957.pdf

19 *MySpace Inc. v. Super Cassettes Industries Ltd* (2016) https://indiankanoon.org/doc/12972852/

20 Supra Note 18

21 *Ibid*

22 https://shellypalmer.com/2023/06/japans-copyright-exception-for-ai-training-data/

23 Artha Dermawan (2023) Text and data mining exceptions in the development of generative AI models https://doi.org/10.1111/jwip.12285

24 https://www.reedsmith.com/en/perspectives/ai-in-entertainment-and-media/2024/02/text-and-data-mining-in-singapore

25 https://www.europarl.europa.eu/RegData/etudes/BRIE/2018/604942/IPOL_BRI(2018)604942_EN.pdf

26 https://www.medianama.com/2025/05/223-india-ai-copyright-law-committee/

CHAPTER 6

Regulation of AI for Healthcare in India

Introduction

Artificial Intelligence (AI) is rapidly transforming the healthcare and life sciences sector in India, offering solutions to major healthcare challenges while driving innovation and efficiency. Its applications span diagnostics, telemedicine, personalised medicine, drug development, clinical imaging, administrative efficiency, mental health, biotechnology, and bioinformatics, creating a paradigm shift in how care is delivered and managed.[1]

The country is witnessing a surge in AI-based startups, research, and collaborations between healthcare providers, technology companies, and government institutions, paving the way for AI-driven innovation. The government's push for National Health Stack, Ayushman Bharat, and Pradhan Mantri Jan Arogya Yojana is helping create the necessary ecosystem for AI-powered healthcare innovations. The US and Europe remain leading markets, while India and China are expanding fast due to large populations and rising digital health adoption. Although regulatory clarity remains a challenge, the market is expected to grow significantly, contributing to both national and global advancements in healthcare AI.

Applications of AI in Healthcare

AI is revolutionising healthcare by enhancing diagnostic accuracy, treatment personalisation, and operational efficiency across the medical ecosystem. By leveraging advanced algorithms and deep learning, AI enables faster, more precise analysis of complex data, leading to better patient outcomes and accelerated medical research.

In diagnostics, AI enables earlier and more precise detection of diseases by analysing imaging, genetic tests, lab results, and clinical notes, directly improving treatment outcomes. Clinical imaging is another key area, where

This chapter has been contributed by Shlok Siddhant – Member, Tanya Kukade – Senior Member, Dr. Milind Antani – Head, Pharmaceutical and Life Sciences Practice, Nishith Desai Associates

deep learning tools detect tumours and other conditions with accuracy and cost-effectiveness that surpass human limits.[2] Similarly, in laboratory testing and clinical microbiology, AI automates processes, improves precision, and guides antibiotic selection, enhancing cure rates.

AI also strengthens drug development by predicting toxicity, shortening trial durations, and improving outcomes.[3] In clinical decision support and precision medicine, it helps design personalised treatments by analysing vast datasets, while predictive modelling forecasts risks and outcomes for proactive care.[4] Robotic surgery highlights its value in enhancing precision, reducing errors, and speeding recovery.

Beyond direct care, AI powers virtual assistants, remote monitoring, and wearables, supporting patient engagement, chronic disease management, and early interventions. In mental health, AI tools aid diagnosis, create tailored treatment plans, and improve accessibility through digital support.[5]

In research, biotechnology, and drug discovery, AI accelerates insights from complex datasets, predicts molecular interactions, and identifies new therapies while optimising clinical trial recruitment and monitoring. It also supports genome editing[6] and bioinformatics, enabling precise DNA modifications, better disease understanding, and personalised therapy development.

Together, these applications demonstrate AI's transformative role across healthcare in India — improving accuracy, efficiency, accessibility, and outcomes while laying the foundation for a more sustainable and equitable system.

Global Regulatory Approaches to AI in Healthcare

Regulators worldwide are working to ensure AI-based medical technologies are safe, ethical, and transparent. While the specifics of regulations may vary, most national regulators are regulating AI based medical technologies as medical devices more specifically software-as-a-medical-device (SaMD), that are standalone applications used to diagnose, treat, or monitor diseases. SaMD is subject to risk assessment, validation, and quality standards to protect patients and maintain accountability.

In the United States, the Food and Drug Administration (US FDA) regulates AI-driven medical technologies as SaMD and has issued multiple guidance documents to cater to the specific requirements of such technologies, including principles on machine learning,[7] transparency,[8] and change control plans.[9] Reports and draft guidance released between 2024[10] and 2025[11] outline how AI can support regulatory decisions while maintaining product safety and effectiveness.

The United Kingdom has taken similar steps, publishing an Evidence Standards Framework for Digital Health Technologies in 2019 which outlines rules for digital health products, including apps, software, and online platforms, whether they are standalone or used in conjunction with other health tools and launching the Software and AI as a Medical Device Change Programme in 2021 to focus on the lifecycle of AI devices.[12] This was followed by a 2022 report titled '*The Regulation of AI as a Medical Device'* released by UK's Regulatory Horizons Council, emphasising communication and patient involvement.

The European Union regulates AI systems under the European Medical Device Regulation and the 2021 AI Act, which establishes rules on risk management, transparency, and oversight. Healthcare AI systems deemed high risk face strict requirements, while low-risk systems like chatbots follow voluntary codes. Critics argue that the Act is too rigid as it cannot adapt to emerging applications.[13]

Regulation of AI for Healthcare in India

In India, AI in healthcare is not yet governed by a single law but instead falls under a web of existing laws, regulations, and guidelines that apply to healthcare and technology. These frameworks, though independent, are adapted to AI use cases in the absence of AI-specific legislation. The Indian regulatory approach is evolving, with an emphasis on ensuring safety, efficacy, and ethical considerations.

Regulation involves several bodies: the Central Drugs Standard Control Organisation (CDSCO) regulates medical devices and drugs, including AI-powered diagnostic and decision-support tools; the National Health Authority (NHA) oversees the Ayushman Bharat Digital Health Mission, where AI is key to telemedicine and digital records; and the Indian Council of Medical Research (ICMR) manages biomedical research, clinical validation, and ethics of AI tools. The Ministry of Health and Family Welfare (MoHFW) drives integration of AI into public health systems, while the Ministry of Electronics and Information Technology (MeitY) regulates digital health technologies more broadly. In addition, the Central Consumer Protection Authority (CCPA) protects consumers from unsafe or misleading AI healthcare products, and the Indian Computer Emergency Response Team (CERT-In) addresses cybersecurity of AI applications.

AI as a Medical Device

AI-based healthcare solutions that meet the definition of a medical device are regulated under the Medical Device Rules, 2017 (MDR), framed under the Drugs and Cosmetics Act, 1940. Devices are classified by risk: Class A (low), Class B (moderate), Class C (high), and Class D (very high). AI-powered devices like imaging systems, diagnostic software, or decision-support systems are generally categorised under moderate risk classes (B or C) depending on their intended use.

Such devices undergo evaluation by CDSCO through clinical investigations, risk assessments, compliance checks, and quality certification before marketing. Software that performs medical functions independently is considered SaMD for the purposes of the MDR and must meet the same safety and efficacy standards as all medical devices. Clinical validation is crucial to ensure accuracy, safety, and reliability of AI-driven diagnostic tools. However, AI-specific challenges like continuous learning, explainability, and ethical implications remain outside the current framework.

Beyond medical device regulation, restrictions apply to AI's direct role in the practice of medicine. Only registered medical practitioners[14] (RMPs) licensed by the National Medical Commission (NMC) may evaluate, diagnose, or manage patients. Since AI cannot hold a license, tools cannot independently provide medical care. The Telemedicine Practice Guidelines, 2020,[15] issued by the NMC, permits AI use as an assistive tool in remote consultations, but always under the supervision of a licensed professional. Responsibility for diagnosis, treatment, and patient outcomes remains with the practitioner, not the AI tool.

Importantly, AI tools are barred from counselling patients or prescribing medicines. While adoption of AI in healthcare is growing, its role remains supportive, and the regulatory framework continues to evolve to keep pace with technological advancements.

Other Applicable Laws

a. *Biomedical Research Framework*

The ICMR has issued Ethical Guidelines for Application of Artificial Intelligence in Biomedical Research and Healthcare,[16] applying to all AI-based biomedical and health research involving human participants and biological data. These emphasise data privacy, informed consent, and data integrity to ensure transparency, ethics, and respect for human rights.

b. Data Protection Framework

India's data protection framework, currently governed by the Information Technology Act, 2000 (IT Act) and its associated rules, is undergoing a significant shift with the introduction of the Digital Personal Data Protection Act, 2023 (DPDPA), which will soon replace the existing regulations. Unlike the previous regime that focused primarily on sensitive personal data, the DPDPA extends protection to all personal data, imposing stricter obligations on digital health businesses. These include requirements around obtaining explicit consent, managing data processing and storage, handling children's data, and regulating cross-border data transfers.

For AI systems processing health data, explicit consent and robust security measures are mandatory, although AI-specific challenges, such as the use of training data, are not directly addressed in the law.

c. Intellectual Property Framework

Intellectual property (IP) protection for AI-driven healthcare is governed by multiple legal frameworks. The Patent Act, 1970 can protect inventions that are novel, non-obvious, and industrially applicable, such as medical devices or software innovations. The Copyright Act 1957, safeguards algorithms, source code, and databases. The Trademarks Act 1999 protects the branding of AI healthcare products, while trade secrets are protected through contractual agreements and provisions under various cyber laws. The proposed Protection of Trade Secrets Bill, 2024 aims to provide clearer rights and remedies in this area.

d. Consumer Protection Framework

The Consumer Protection Act, 2019 (CPA) provides for the protection of consumers' interest and establishes a redressal mechanism. It imposes multiple responsibilities upon sellers and service providers, including the prohibition of unfair trade practices, misleading advertisements and establishes a product liability regime. Central Consumer Protection Authority (CCPA) is the regulatory body under the CPA that presides over the administration of the CPA and issues penalties. AI systems can pose risks, especially if they malfunction or cause harm to users or third parties. Depending on the harm caused by defective AI systems, the company may be held liable under the CPA. Product liability provision under CPA would be triggered in case of harm caused due to defective design, implementation, or data breaches.

e. Antitrust Framework

The Indian antitrust framework is governed by the *Competition Act, 2002*, which seeks to protect consumer interests by preventing practices that harm fair and healthy competition in India. The Act primarily addresses anti-competitive behaviours and potentially anti-competitive combinations. The Competition Commission of India (CCI) functions as the regulator under

this law. Importantly, the Competition Act follows an *ex-post* approach, where the CCI examines whether an agreement or action has had an *appreciable adverse effect on competition (AAEC).* This assessment may occur either on the basis of a complaint or through *suo moto* action initiated by the CCI.

To more effectively address the complexities of digital markets, the Digital Competition Bill, 2024 (also referred to as the Digital Competition Law) has been proposed. Unlike the existing Competition Act, this Bill adopts an *ex-ante* approach, meaning it prescribes specific guardrails within which companies must operate to deter anti-competitive conduct in advance. Although the Bill has yet to be finalised and brought into force, it is expected to have far-reaching implications, including for AI-driven medical technologies.

Potential Anti-Competitive Behaviours in AI Healthcare

Under the competition law framework, AI-based medical technology companies may, whether intentionally or inadvertently, engage in behaviours that could be considered anti-competitive. These include:

- ***Tying Arrangements****:* Forcing customers to purchase additional services or products as a condition of accessing a primary product. For instance, a hospital software package that obliges customers to also buy AI-powered diagnostic tools, limiting market entry for competitors.

- ***Predatory Pricing***: Setting prices below cost to eliminate competition, with the intention of raising prices once competitors exit the market. For example, offering AI-powered healthcare solutions free of cost to initially drive out rivals.

- ***Data Hoarding***: Restricting access to essential health data that competitors need to train or improve AI models. Proprietary patient data held exclusively by one company can create significant barriers to market entry.

- ***Unfair or Discriminatory Contract Terms****:* Imposing exclusive-use requirements on healthcare providers that prevent them from adopting competitors' products. Such contracts may include financial penalties or restrictive conditions, effectively locking providers into a single supplier's ecosystem.

These practices, if left unchecked, can reduce competition, limit innovation, increase costs, and ultimately harm consumers. As a result, they may attract regulatory scrutiny and legal action under the existing Competition Act or the forthcoming Digital Competition Law.

Challenges in Regulating AI in India

The regulation of AI as a medical device in India poses unique challenges, as existing rules were designed for traditional, static devices, not dynamic and adaptive AI systems.

- The CDSCO has recognised AI-driven medical devices as SaMD and issued risk classification guidance, but without specific relaxations, compliance remains difficult.
- Licensing requires adherence to quality management standards and sales from licensed premises, which is impractical for software distributed digitally.
- Clinical investigations are also mandated for novel devices, yet no AI-specific guidance exists, creating uncertainty.
- Post-approval changes under the MDR — major (requiring approval) or minor (requiring notification) — are poorly suited to AI systems that evolve frequently, potentially triggering constant regulatory updates.
- Labelling requirements under MDR and The Legal Metrology (Packaged Commodities) Rules 2011 also pose challenges, since AI-driven SaMD lacks a physical label.
- Pricing restrictions under the Drug (Prices Control) Order 2013, including caps on annual increases and mandatory submissions to the National Pharmaceutical Pricing Authority, add further burdens for software-based products.
- Advertising rules also constrain AI developers: misleading claims can render products misbranded, and the Drugs and Magic Remedies (Objectionable Advertisements) Act 1954 prohibits claims for many conditions — such as cancer, diabetes, and heart disease — even though many AI tools target these disorders.
- The Uniform Code for Marketing Practices in Medical Devices regulates promotional activities and interactions with healthcare professionals (HCPs), limiting training and education. Since AI-driven SaMD often requires detailed and periodic training for HCPs, such needs risk bringing the promotional activities undertaken by AI-driven companies under scrutiny.

Ethical & Legal Risks of AI in Healthcare

i. *Bias and Discrimination*: AI models can inherit biases from training data, leading to discriminatory outcomes in healthcare. This risks unequal treatment for certain groups, worsens health disparities, and undermines trust in AI-driven systems.

ii. *Quality of Data:* The performance of AI systems depends on large, diverse datasets. Without *comprehensive* data, predictions may be skewed or

inaccurate.[17] Errors in defining relevant metrics can mislead algorithms, and AI lacks the clinical intuition of human providers, making human oversight essential.[18]

iii. *Doctor-Patient Relationship:* Increased reliance on AI may weaken empathy and trust within the doctor-patient relationship. Patients could feel alienated if AI takes a larger role in decision-making, reducing the importance of human judgment.

iv. *Privacy and Confidentiality:* AI and big data create significant risks to patient privacy. Protecting *sensitive* data is ethically and legally necessary to maintain trust, autonomy, and compliance. Strong regulation is essential to safeguard confidentiality.[19]

v. *Physician Preparedness:* Widespread adoption of AI requires substantial training and *awareness* among physicians. Barriers such as limited access to technology, language gaps, and lack of expertise — especially in rural areas —must be addressed.

vi. *Cybersecurity*: AI-driven healthcare systems face growing vulnerability to cyberattacks, which can compromise sensitive data, disrupt care, and endanger patient safety.

vii. *Environmental Impact*: Training and deploying complex AI models requires large amounts of *computational* power and energy, often from non-renewable sources. This contributes to higher carbon emissions and strains energy resources.

Future Technologies beyond SaMDs

i. *Virtual Reality and Augmented Reality in Medical Training and Education:* VR and AR are transformative in medical training, simulating real-world scenarios for risk-free practice. VR enables surgery simulations and skill-building, while AR overlays patient information during training and supports precision in surgeries. VR also aids in pain management and rehabilitation. Despite benefits, challenges include high costs, limited access, and ensuring effective transfer of skills to clinical practice.[20]

ii. *Robotics in Healthcare:* Robotics spans service, assistive, socially assistive, teleoperated, and interventional uses. Robots handle tasks, aid mobility, provide companionship, enable remote care, and assist in minimally invasive surgeries. Assistive robotics includes prosthetics, orthotics, and exoskeletons, with advances in sensors and control systems enabling bionic limbs. Challenges remain in high costs, integration, and resistance from providers and patients, making transparency and training essential.[21]

iii. *Nanotechnology in Diagnostic Imaging and Drug Delivery:* Nanotechnology enables targeted drug delivery and improved imaging. Nanoscale systems enhance treatment outcomes by reducing side effects, while nanoparticles improve imaging resolution and specificity. Examples include liposomes delivering chemotherapy and gold nano-shells for cancer diagnostics.

Concerns persist about toxicity and safety, requiring strict evaluation and regulatory guidance.[22]

iv. *3D Printed Organs:* Organ shortages drive innovations like microfluidics, organ-on-chip models, and 3D printing. 3D printing shows the most promise, creating tissues with vascular structures using imaging data and biomaterials. Researchers have printed biomimetic tissues like hearts and kidneys, though full organs remain in development. Success depends on bioinks, vascular networks, and evolving regulations.[23]

v. *Predictive analytics in healthcare*: Predictive analytics improves outcomes, efficiency, and proactive care through early detection, chronic disease forecasting, and personalised treatments. It optimises operations and engages patients with risk assessments and reminders. Challenges include privacy, bias, interpretability, and integration with health records. Emerging AI tools and federated learning may improve accuracy while protecting privacy.[24]

vi. *Personalised Medicine:* Personalised medicine tailors care using genetic, environmental, and lifestyle factors. It supports early detection, reduces drug complications, and optimises treatments, especially in oncology and cardiology. While it lowers costs by avoiding trial-and-error approaches, challenges include expenses, limited access, and specialised knowledge needs. Advances in genomics and regulations are making it more accessible, offering safer and individualised treatments.[25]

Conclusion

The integration of AI into healthcare can revolutionise patient care, improve efficiency, and advance research, but it also raises significant legal and ethical challenges. Existing laws on data protection and medical devices must adapt to AI's distinct issues, particularly around liability, accountability, and intellectual property. Responsibility in cases of harm, transparency, and patient trust remain central concerns.

Unregulated AI in healthcare poses serious risks that cannot be ignored. Bias and discrimination may be perpetuated by algorithms trained on unrepresentative data, leading to unequal treatment of patients and worsening health disparities. Diagnostic errors can go undetected if AI tools are not rigorously validated, endangering patient safety. The lack of transparency in decision-making undermines the doctor-patient relationship, as neither patients nor clinicians may fully understand how conclusions are reached.

Moreover, data privacy is at significant risk, with sensitive patient information potentially exposed or misused due to inadequate security measures. From a market perspective, unregulated environments may encourage monopolistic practices like data hoarding or unfair tying arrangements, restricting competition and innovation.

The need of the hour is robust and adaptive regulations that ensure AI-driven healthcare solutions are safe, ethical, and accountable. Regulatory frameworks should establish risk-based classification, mandatory clinical validation, strict data protection rules, and continuous monitoring mechanisms to manage AI's evolving nature. Clear guidelines on liability, transparency, and informed consent are essential to protect patient welfare, promote equitable outcomes, and maintain public trust.

As AI evolves, legal frameworks and ethical guidelines must keep pace. Collaboration among policymakers, healthcare providers, technology developers, and civil society is critical to ensure that AI strengthens healthcare systems without compromising safety, equity, or fundamental rights. Only a comprehensive, well-regulated approach can enable India to realise AI's immense promise while setting a global precedent for responsible and equitable adoption in healthcare.

Endnotes

1 Accessible at: https://pubmed.ncbi.nlm.nih.gov/34286183/. (Last accessed September 04, 2025)

2 Accessible at: https://pmc.ncbi.nlm.nih.gov/articles/PMC2464549/. (Last accessed September 04, 2025)

3 Accessible at: https://www.researchgate.net/publication/355069925_Applications_of_Artificial_Intelligence_AI_in_healthcare_A_review. (Last accessed September 04, 2025)

4 Accessible at: https://pmc.ncbi.nlm.nih.gov/articles/PMC11141850/. (Last accessed September 04, 2025)

5 Accessible at: https://www.tandfonline.com/doi/epdf/10.2147/RMHP.S461562?needAccess=true. (Last accessed September 04, 2025)

6 Accessible at: https://www.researchgate.net/publication/379113749_Applications_and_Challenges_of_Artificial_Intelligence_in_Life_Sciences. (Last accessed September 04, 2025)

7 Available at: https://www.fda.gov/medical-devices/software-medical-device-samd/good-machine-learning-practice-medical-devicedevelopment-guiding-principles. (Last accessed September 04, 2025)

8 *Ibid*

9 Available at: https://www.fda.gov/regulatory-information/search-fda-guidance-documents/marketing-submission-recommendationspredetermined-change-control-plan-artificial-intelligence. (Last accessed September 04, 2025)

10 Available at: https://www.fda.gov/media/177030/download?attachment. (Last accessed September 04, 2025)

11 Available at: https://www.fda.gov/regulatory-information/search-fda-guidance-documents/considerations-use-artificial-intelligence-support-regulatory-decision-making-drug-and-biological. (Last accessed September 04, 2025)

12 Accessible at: https://www.gov.uk/government/news/mhras-ai-regulatory-strategy-ensures-patient-safety-and-industry-innovation-into-2030 and https://pmc.ncbi.nlm.nih.gov/articles/PMC10930608/#sec4-healthcare-12-00562. (Last accessed September 04, 2025)

13 *Ibid*

14 A registered medical practitioner is an individual duly registered with the National or State Medical Council to obtain a license to practise medicine in India.

15 Accessible at: https://esanjeevani.mohfw.gov.in/assets/guidelines/Telemedicine_Practice_Guidelines.pdf. (Last accessed September 04, 2025)

16 Accessible at: https://www.icmr.gov.in/ethical-guidelines-for-application-of-artificial-intelligence-in-biomedical-research-and-healthcare (Last accessed September 04, 2025)

17 Accessible at: https://pmc.ncbi.nlm.nih.gov/articles/PMC8285156/. (Last accessed September 04, 2025)

18 Accessible at: https://www.researchgate.net/publication/377091459_The_Integration_of_Artificial_Intelligence_into_Clinical_Practice. (Last accessed September 04, 2025)

19 Accessible at: https://www.researchgate.net/publication/378288596_AI_in_Data_Privacy_and_Security. (Last accessed September 04, 2025)

20 Accessible at: https://www.jmir.org/2021/2/e25499/. (Last accessed September 4th, 2025)

21 Accessible at: https://link.springer.com/article/10.1007/s42979-023-02551-0. (Last accessed September 04, 2025)

22 Accessible at: https://pmc.ncbi.nlm.nih.gov/articles/PMC7953199/. (Last accessed September 04, 2025)

23 Accessible at: https://pdf.sciencedirectassets.com/320498/1-s2.0-S2590183424X00022/1-s2.0-S2590183424000127.

24 Accessible at: https://www.researchgate.net/publication/384148771_Healthcare_Data_Analytics_and_Predictive_Modelling_Enhancing_Outcomes_in_Resource_Allocation_Disease_Prevalence_and_High-Risk_Populations (Last accessed September 04, 2025)

25 Accessible at: https://www.researchgate.net/publication/354269399_Personalized_Medicine_A_Review. (Last accessed September 04, 2025)

CHAPTER 7

Cyber Threats in the Age of AI: Securing the Digital Frontier

Introduction

Artificial intelligence (AI) is fundamentally altering the landscape of cybersecurity. In the past, digital assaults were burdensome, manual efforts limited by human scale and creativity. Today, AI enables adversaries to scale attacks, personalise deception, and outpace defence systems. AI likewise aids defenders by letting them find threats in real time, respond to them in a flexible way, and search for threats that might happen in the future. The resultant dynamic is not just evolution; it's a cyber arms race where speed, scale, and intelligence are the main points of contention.

Current empirical data support this transformation. According to the World Economic Forum's Global Cybersecurity Outlook 2025, the average incidence of cyberattacks per week on each organisation rose from 818 in Q2 2021 to 1,984 in Q2 2025. This is more than double and a 58 percent jump over two years.[1]

Aon's 2025 Cyber Risk Report asserts that the number of incidents in the Asia-Pacific region went up 29 percent from 2020 to 2024 and 134 percent overall from 2020 to 2024. The report additionally indicates that AI-fueled deepfakes and social-engineering campaigns have intensified significantly, with social-engineering instances up 53 percent from the previous year and allegations associated with those up 233 percent.[2]

However, these figures only give a hint of the bigger change that is happening. The basic idea of attack and defence is changing. AI lets perpetrators automate and improve not only a larger number of phishing emails but also phishing that changes to fit a person's profile in real time. It also lets them create

This chapter has been contributed by Sohom Banerjee, Senior Research Associate and Ayan Bhattacharjee, Research Associate, CUTS International

polymorphic malware that changes all the time to avoid being found. An experienced attacker could use a network of AI-powered bots to look for weaknesses, execute targeted attacks, move laterally, and steal data with little help from other individuals.

On the defence side, AI is becoming indispensable. Security operations centres (SOCs) presently analyse and compare huge amounts of telemetry data, such as logs, packet intercepts, and endpoint indicators. They use machine learning to find small changes that human analysts might miss. Behaviour-based models find vulnerabilities from within or fraudulent use of credentials. Automated response mechanisms can quickly isolate systems that have been hacked, undo changes, or apply patches. In a way, defenders are increasingly looking for AI to help people make decisions.

This collision of AI and cybersecurity is especially consequential for India. India's digital ecosystem is massive and rapidly evolving across fintech, e-governance, telecom, critical infrastructure, health, and education. However, scale also means vulnerability. An attack on public infrastructure or financial systems can affect millions of people, breaking trust, causing services to stop working, and even causing national security problems.

In recent years, India has witnessed high-impact cyber incidents, whether via malware targeting banks or large-scale data leaks involving citizen identity systems. These events underscore the peril that lies in delaying adaptation. As defenders grapple with traditional patches and perimeter defences, adversaries deploying AI-driven tools increasingly exploit gaps: unpatched systems, weak identity management, supply-chain vulnerabilities, and the human element.

More troubling is the widening gap in capacities. The widening gap in skills is even more worrying: India, just like many other countries, doesn't have enough cybersecurity experts who know how to use AI. Also, regulatory and institutional inertia could mean that governance structures don't keep up with new threats. Absence of AI-aware regulation that looks ahead, enemies may be able to act with little fear of punishment, while defenders are held back by legal, procedural, or coordination issues.

This chapter positions itself at the interface of technology, security, and policy. It explores how AI amplifies cyber threats (from advanced phishing to autonomous exploits and deepfakes), and how AI can power defence (real-time detection, model-based threat intelligence, automated mitigation). Then, through global and Indian case studies, it examines vulnerabilities intrinsic to India's infrastructure and institutional landscape. Finally, it offers integrated regulatory and technological recommendations to equip India for this new era.

AI-Enhanced Cyber Threats

AI-Powered Social Engineering

The perpetrators are employing AI to make social engineering fraud much worse. Fraudsters depend on automated voice cloning tools like ElevenLabs and Resemble to mimic a victim's acquaintance with minimal voice samples, bypassing the victim's scepticism. In India, criminals have used cloned voices in WhatsApp messages and phone calls to dupe users into transferring funds.

An inquiry by the Indian Express in 2025 found many AI-driven fraudulent activities, such as voice cloning scams, one-time-password (OTP) extraction through AI-based call merging, spear-phishing emails made by sophisticated large language models (LLMs), counterfeit "police arrest" footage backdrops, forged loan applications, misleading investment platforms, romance scams, and deepfake extortion videos.[3]

All these fraudulent activities take advantage of sentiments and faith. AI-powered fraud takes advantage of how people think. It makes pleas appear real and pressing. Global cases underscore this trend. In one widely reported incident, criminals staged a deepfake video conference by "cloning" senior executives of a UK engineering firm, prompting a transfer of US$25mn. In a separate attempt, scammers used a synthetic voice purporting to be Ferrari's CEO — most employees were fooled, though one verification check prevented the loss.[4]

Likewise, an employee in another case authorised a €220,000 transfer after receiving an AI-cloned call that appeared to come from their own CEO.[5] These episodes illustrate how deepfake video and voice attacks have moved from novelty to high-stakes corporate fraud.

These episodes show that deepfakes have moved from novelty to a standard weapon in criminal toolkits. Firms struck by such frauds have, on average, suffered a 27 percent decline in market value.[6]

In India, threat actors are actively using deepfake technologies to produce highly persuasive malicious content, markedly elevating the sophistication of social-engineering campaigns. AI now personalises deception with uncanny fidelity, cloning a relative's voice, fabricating convincing video messages, drafting bespoke phishing copy, or masquerading as trusted chatbots on counterfeit apps. This weaponisation of AI erodes public trust in digital communications and poses immediate risks to individuals, businesses, and public institutions.[7]

AI-Augmented Malware and Attacks

Beyond social tricks, AI is also enabling autonomous cyberattacks. Malicious code can now use machine learning (ML) to optimise its own behaviour and evade defences. Researchers warn that next-generation malware will dynamically change its code to evade detection and self-learn during attacks.[8]

There are already reports of hackers using AI to write and optimise malware. For example, Anthropic (the maker of the Claude chatbot) revealed that cybercriminals have "weaponised" its AI, using it to generate malicious code for at least 17 organisations. Generative AI can also be used to discover novel exploits. Attackers feed code libraries into LLMs to brainstorm zero-day attack vectors or to generate obfuscated encryption schemes. Advanced bots can automatically scan millions of devices for vulnerabilities and trigger tailored exploits at network speed. Today's adversaries can craft highly targeted phishing emails, probe for weaknesses at scale, and launch automated attacks that adapt in real time.[9]

These developments effectively lower the skill bar for potent attacks. Small criminal groups or state-sponsored hackers can use off-the-shelf AI tools to mount campaigns of unprecedented scale. Autonomous attack engines ("AI cyberweapons") could potentially spread through networks like worms, optimise ransomware demands, or even coordinate multi-vector assaults (e.g. simultaneous attacks on IoT, cloud and operational systems).

The blurring of cyber and physical threats is also rising. AI-driven malware could target industrial control systems with speed and stealth, threatening critical infrastructure. Analysts warn that AI-driven cyber weapons will evolve faster than defenders' signatures, making timely detection very challenging.

Deepfakes and Disinformation

A related threat is the use of AI for influence operations and fraud beyond financial scams. Deepfake videos and audios can be deployed *en masse* to spread misinformation, sway public opinion, or incite panic. In the Indian context, deepfake content has already been used to create fake speeches and election propaganda. For example, intelligence agencies have observed deepfake videos of public figures used in disinformation campaigns designed to sow unrest.[10]

Globally, the risk extends to automated creation of "fake news" or fraudulent endorsements. Without strong AI countermeasures, deepfakes could be weaponised for *cyberwarfare* or election interference.

Vulnerabilities in India's Cyber Infrastructure

India's rapidly expanding digital ecosystem presents both opportunities and risks. With an internet user base approaching 900 million, India is building a vast online economy and e-governance infrastructure.[11] However, this scale also means a large attack surface. An increasingly large and digitised economy, India is a bigger target than many.[12]

India now ranks in the top 10 globally for cybercrime (Oxford Cybercrime Index), and its National Cybersecurity Coordinator reports ransomware payouts doubling from 2022 to 2023, with India experiencing nearly twice the global average rate of cyber incidents. These headline figures are symptoms of deeper structural weaknesses. India's exposure is amplified by:

Critical Infrastructure Exposure

Key sectors such as power grids, healthcare systems, financial networks – have already seen cyberattacks. The Stimson Centre reports multiple incidents. Attackers have penetrated an atomic power plant control network, disrupted a major hospital's operations, and shut down parts of Mumbai's power grid. These intrusions often exploit unpatched systems or weak network segmentation. State and non-state groups have greater access to sophisticated tools like AI that personalise phishing against India's infrastructure.[13]

In finance, a landmark breach saw Rs 94 crore (USD 13.5/ million) stolen from Cosmos Bank via cyberattacks on its ATM systems. Another massive leak exposed Aadhaar biometric data of over a billion Indians for sale.[14] Such breaches highlight that even established institutions (banks, ID systems) have exploitable vulnerabilities.

Regulatory and Policy Gaps

India's first National Cyber Security Policy dates to 2013 and has not kept pace with AI-era threats. There is no unified AI strategy for security, and laws have lagged behind the technology. The legal framework (IT Act and RBI Guidelines) offers limited guidance on AI-enabled crime. Until recently, incident reporting requirements were lax; only in 2023 did CERT-In mandate stricter breach reporting (within 6 hours for certain events) and broaden its purview. Proposed updates, such as the draft Digital India Act, aim to modernise IT law and may introduce "no-go zones" for harmful AI applications.[15]

CERT-In has also begun issuing voluntary "AI Bill of Materials" (AIBOM) guidelines to encourage transparency in AI systems.[16] These steps signal intent, but enforcement remains a challenge.

Talent and Awareness Shortage

India lacks enough AI-literate cybersecurity professionals. Observers warn of an AI-skills gap. Traditional security teams often cannot use AI tools effectively for defence. Without rapid upskilling, India risks slower breach response, compliance failures and an erosion of its cyber-sovereignty.[17]

India needs over 1.5 million cyber professionals, with a 30 percent shortage today.[18] This shortage hampers both threat hunting and building robust AI systems. Public awareness is also low. McAfee found nearly half of Indians cannot distinguish an AI voice from a human one, making social-engineering attacks easier.

Supply-Chain Risks

India's tech ecosystem is global, but this interdependence can import risks. Hardware, software and cloud platforms often originate from multinational vendors. A vulnerability or backdoor in a widely used system (e.g. an IoT OS or an AI library) can propagate quickly. Recognising this, CERT-In's new guidelines emphasise Software Bill of Materials (SBOM) and AI Bill of Materials (AIBOM). They recommend companies enumerate every component – software libraries, datasets, hardware modules – used in products.

The AIBOM specifically calls for disclosure of AI model details, training data sources, performance metrics and known biases. Although voluntary, such transparency can help identify hidden weaknesses (for example, adversarial biases) before they are exploited. Over time, adherence to SBOM/AIBOM practices is likely to become a *de facto* requirement in contracts and regulations, bolstering supply-chain security.

So, India's vulnerabilities stem from rapid digital growth outpacing governance and skill development. The nation's critical sectors, from banking to energy, face both conventional hacking and novel AI-driven threats. Attacks have already disrupted vital services and shaken public trust. To safeguard national security and economic interests, India must shore up its defences across technology, institutions and law.

AI for Cyber Defence

The same AI that powers attacks can and must power defence. Leading cybersecurity providers and governments are now integrating AI into protective systems at scale. The basic principle is leveraging AI's pattern-recognition and automation strengths to detect anomalies faster than humans alone can. For example, modern security operations centres (SOCs) use ML to analyse millions of logs per second, spotting the faint signature of a breach in real time.

Advanced "user behaviour analytics" can learn normal patterns and flag deviations that might indicate insider threats or compromised credentials. AI can also speed up incident response. Automated playbooks can quarantine affected devices or roll back malicious changes within seconds of detection.

In India, both industry and government are piloting AI defences. Firms are now under pressure (from insurers and regulators) to adopt advanced AI monitoring and regular security audits. Startups are emerging to meet this need. For example, in early 2025, Zero Defend Security launched Vastav AI, India's first deepfake-detection platform.[19]

Vastav AI uses deep learning and forensic analysis to vet media; it highlights suspicious regions in videos/images and assigns confidence scores to authenticity. Such tools exemplify how defenders use AI: making the invisible visible. By surfacing metadata anomalies or heatmaps of tampering, Vastav AI and similar systems help human analysts trust and act on AI judgments. More broadly, AI-driven computer vision and voice analysis can flag synthetic content on Indian social networks, aiding law enforcement in curbing disinformation campaigns.

On the corporate side, major vendors have begun embedding AI into security products. Check Point and other firms report using AI "copilots" for threat hunting and automated patching. Microsoft, Google and others now offer automated threat analytics services (often in the cloud) that harness massive compute and global data to predict attacks. Governments, too, are investing; the U.S. Department of Defense has contracted OpenAI to improve its AI-based cyber defences, and similar R&D partnerships are forming worldwide. Although India's military and intelligence agencies operate classified programmes, public-private initiatives (like CERT-In's vulnerability analysis centres) are increasingly experimenting with AI-assisted anomaly detection on critical networks.

Despite these advances, AI defence has limits. Pure "black-box" AI models can be brittle under adversarial attack – for instance, subtle "poisoning" of AI training data by an attacker can induce misclassifications. Explainability is also critical, security teams need to understand *why* an AI flagged an event to avoid false alarms. This is why tools like Vastav emphasize interpretability. In practice, experts recommend keeping humans in the loop – using AI for triage and prioritisation but leaving final response decisions to trained personnel. Building an "AI-augmented workforce" is therefore key. Security analysts need skills in ML, statistics and cloud infrastructure as much as in traditional network defense. Accordingly, the challenge isn't 'more AI' but 'better integration', human-in-the-loop operations embedded within defense-in-depth.

Integrated Regulatory and Technical Approaches

Facing AI-driven threats requires more than technology alone. India must adopt integrated policies that align legal, technical and international efforts. Several strands of regulation and governance are pertinent:

National Cybersecurity Strategy

India's core cyber strategy was last updated in 2013, long before AI became pervasive. Recognising this, the government is now drafting a new framework. In 2023, CERT-In issued strengthened incident-reporting directives and in parallel, NCIIPC published the *National Cyber Security Reference Framework* (NCRF). The NCRF focuses on the seven most critical infrastructure sectors (banking, energy, telecom, transport, healthcare, strategic enterprises, government) where threats have spiked. It mandates roles and responsibilities across agencies, improving coordination. Future strategy updates must explicitly address AI. This could include classifying AI-driven cyberattacks as a high-priority threat and integrating AI red-teaming into standard security exercises.

Data Protection and AI Ethics

AI systems rely on data. India's Personal Data Protection legislation (the DPDP Act, 2023) provides data-use norms that indirectly affect AI developers. However, specific guidelines on AI ethics and safety are still evolving. NITI Aayog's "Principles for Responsible AI" (2021) encourages fairness, accountability and explainability in AI development.

Going forward, regulations may require critical AI systems (for example, those in finance or government) to undergo third-party audits for robustness and bias mitigation. Internationally, frameworks like the forthcoming EU AI Act categorise AI by risk level. India could adopt similar risk-based regulation for AI, especially for surveillance and deepfake generation.

Cybersecurity Regulations and Standards

India has long-standing laws (IT Act, RBI regulations) on cyber fraud and privacy, but new threats call for updates. One promising development is CERT-In's BOM (Bill of Materials) Guidelines of 2025. These guidelines define categories like SBOM (Software BOM), AIBOM (AI BOM), etc., and encourage organisations to inventory all components in software, hardware and AI systems.

The AIBOM is especially noteworthy. It would require disclosing AI model architectures, training datasets, performance metrics and security features. This kind of transparency can expose hidden vulnerabilities (for example,

outdated ML libraries or unverified data sources) before they are exploited. Currently voluntary, AIBOM-like practices may soon be mandated for critical sectors or government procurement.

Alongside, India is developing Indian Standards for AI risk management (BIS is adopting ISO AI guidelines). Incorporating such standards into procurement and certification regimes will raise the baseline security of AI products.

Sectoral Regulations

Financial, telecom and other sectors must update their rules for AI. For instance, TRAI's 2023 recommendations propose an independent AI authority and risk categorisation of AI applications. Banks and payment networks (Regulated by RBI) should require strong AI audit trails for automated trading and loan approval algorithms.

Similarly, as deepfake scams increasingly target e-governance, the government should mandate secure multi-factor authentication and verifiable "trusted channel" communications for critical transactions. In 2024, the Reserve Bank of India already flagged cybersecurity and legacy technology as top banking risks,[20] and regulators could now emphasise AI-proofing as part of banks' compliance obligations.

International and Multi-Stakeholder Initiatives

Cybersecurity is inherently cross-border. India participates in forums like the UN Group of Governmental Experts on Lethal Autonomous Weapons (though AI cyberweapons are not yet specifically regulated). More practically, India is engaged in Quad and bilateral dialogues on cybersecurity. These forums are now discussing AI, for example, a recent Quad joint statement calls for cooperation on AI security and resilience. India should leverage such alliances to share threat intelligence on AI-enabled attacks and to harmonise norms (for example, attribution standards, corporate transparency agreements).

Public–private partnerships will also be vital. The World Economic Forum notes that skill shortages in cybersecurity can be addressed by multi-stakeholder "talent pipelines". India's government can collaborate with industry to create AI-defence training programmes and certification courses, analogous to initiatives like the Forum's Cybersecurity Skills Consortium. Finally, legal cooperation is needed to prosecute AI-driven crimes: building capacities in cyber forensics and negotiating mutual legal assistance treaties that cover emerging AI evidence (for example, recovery of LLM logs or metadata from cloud services).

Collectively, these regulatory and technical measures form an integrated defence posture. No single law or gadget will suffice; instead, India needs a comprehensive framework that spans legislation, standard-setting, enforcement, and capacity-building, all attuned to the new AI-driven landscape.

Recommendations

India's exposure to AI-enabled cyber risk is now systemic. Attack volumes are rising, attack quality is improving through deepfakes and automation, and the blast radius spans citizens, critical infrastructure, and the economy. Meeting this moment requires a **socio-technical, whole-of-nation** response that aligns law, institutions, markets, and technology, not a tools-only fix. India should pursue a multi-pronged strategy. Key recommendations include:

Update National Strategy

Revise the national cyber policy to explicitly address AI threats. This should involve (a) classifying AI-powered attacks as a high-priority risk, (b) mandating AI-aware incident response playbooks, and (c) funding AI-defence R&D. For example, the government could establish an "AI in Cybersecurity" task force under the National Cyber Security Coordinator to coordinate strategy and public outreach.

Strengthen Regulations and Standards

Implement and enforce the new BOM guidelines, making SBOM/AIBOM compliance mandatory in critical infrastructure (banks, utilities, healthcare). Accelerate passage of the Digital India Act and ensure it contains clear provisions on AI accountability (e.g. penalties for deceptive deepfakes). Align Indian data laws with global norms to ensure the availability of anonymised datasets for security research, while protecting personal privacy. Encourage or require independent audits of AI systems used in sensitive roles (finance, election tech, public services), like how financial auditors check accounting.

Enhance Cyber Workforce

Invest in training programmes to produce cybersecurity professionals skilled in AI. Update academic curricula to include hands-on AI security modules (such as adversarial ML and secure coding). Support industry-led apprenticeship programmes (for example, incentivise IT companies to set up AI-cyber labs on campuses). Public awareness campaigns should also highlight AI-fraud risks and defences, empowering citizens to recognise deepfakes and phishing attempts.

Foster a Competitive Cyber Ecosystem

Promote a diverse cybersecurity industry by supporting startups and SMEs developing AI-based defence tools. Use government procurement to give a leg up to domestic vendors (when security merits) and require open standards to avoid vendor lock-in.

Emphasising data portability and interoperability could diffuse the risks posed due to the concentrated digital platform market.

Public–Private Collaboration

Create an India-wide AI-threat intel sharing alliance. Build on CERT-In and sectoral Information Sharing & Analysis Centres (ISACs) by integrating AI-threat data feeds. For instance, finance and energy firms could share unusual AI-generated scam indicators in real time. Government agencies should streamline reporting for AI cyber incidents to speed up collective learning (for example, a centralised AI incident registry). Encourage cross-sector "red teaming" exercises involving both government and private organisations to simulate AI-augmented attack scenarios.

International Engagement

Advocate in global forums for norms on malicious AI. This might include pushing for an international pledge (akin to the Paris Call) against weaponising AI for illicit hacking or influence operations. In bilateral dialogues (with the U.S., EU, Japan, among others), negotiate agreements on disclosure of AI malware signatures and joint attribution of state-sponsored AI-cyberattacks. Collaborate with technology-export partners to ensure that India has access to secure AI technologies (for example, high-end chips) and to prevent the proliferation of AI capabilities to adversaries.

By integrating these policies, India can turn AI from a pure threat vector into a strategic advantage. The government should not only see AI through the lens of cutting-edge innovation but also through that of robust governance. A balanced approach, encouraging AI adoption while setting clear rules for safe and fair use will help safeguard critical services and national security.

Conclusion

AI is transforming cyberspace at breakneck speed. In this new era, every element of digital defence must evolve. Attackers wield AI to create more convincing frauds and to automate assault campaigns; defenders must counter with AI-powered vigilance and smarter regulation. For India, the stakes are high. A vast population, a growing digital economy and a complex security environment leave little margin for error. However, opportunities exist. By

investing in talent, enforcing transparency, and crafting agile policies, India can build a cyber-resilient society.

Above all, securing the digital frontier will require a whole-of-nation effort. Lawmakers, industry leaders and technologists must collaborate to ensure that AI bolsters India's cyber defences rather than undermining them. With the right safeguards, the country can protect its citizens and infrastructure from AI-amplified threats, while harnessing AI to maintain a strategic edge. The urgent consensus is clear: in an AI-driven world, preparedness and innovation must go hand in hand.

Endnotes

1 Willige, A. (2025, September 30). *Cybersecurity awareness month: 10 things to know in 2025.* World Economic Forum. https://www.weforum.org/stories/2025/09/cybersecurity-awareness-month-cybercrime-ai-threats-2025/

2 Bolima, D., M. (2025). *Aon's 2025 cyber risk report highlights rising AI-driven attacks.* Cybersecurity Asia. https://cybersecurityasia.net/aons-2025-cyber-risk-report-rising-ai-attack/

3 Deshkar, A. (2025, September 7). *AI scams surge in India: Voice cloning, deepfakes and OTP frauds leave victims helpless*. The Indian Express. https://indianexpress.com/article/technology/artificial-intelligence/ai-scams-surge-in-india-voice-cloning-deepfakes-and-otp-frauds-leave-victims-helpless-10232064/

4 Supra Note 3

5 Allen, J. M. (2025, September 10). *The rise of the AI-cloned voice scam*. American Bar Association. https://www.americanbar.org/groups/senior_lawyers/resources/voice-of-experience/2025-september/ai-cloned-voice-scam/

6 The Economic Times. (2025, August 6). *AI-driven cyber-attacks surge in India and APAC, warns cyber risk report*. ETCFO. https://cfo.economictimes.indiatimes.com/news/ai-driven-cyber-attacks-surge-in-india-and-apac-warns-cyber-risk-report/123139419

7 Supra Note 5

8 Izrael, N. (2024, November 14). *The rise of AI weapons, zero-days, and state-sponsored chaos.* Armis. https://www.armis.com/blog/the-rise-of-ai-weapons-zero-days-and-state-sponsored-chaos/

9 Shukla, P. (2025, September 27). *AI talent gap threatens India's cyber security*. BW Security World. https://bwsecurityworld.com/technology/ai-talent-gap-threatens-indias-cyber-security/

10 Cyble. (2025, May 8). *How deepfake threats are reshaping security strategies in the India region.* Cyble. https://cyble.com/knowledge-hub/deepfake-threats-india-security-strategies/

11 India Brand Equity Foundation. (2025, January 17). *India's internet users to exceed 900 million in 2025, driven by Indic languages.* IBEF. https://ibef.org/news/india-s-internet-users-to-exceed-900-million-in-2025-driven-by-indic-languages

12 Devanny, J., & Laudrain, A. P. B. (2025, March 27). *Interpreting India's cyber statecraft*. Carnegie Endowment for International Peace. https://carnegieendowment.org/research/2025/03/interpreting-indias-cyber-statecraft?lang=en

13 Basu, A. (2025, September 25). *Assessing cyber risks and resilience in India and Pakistan*. Stimson Center. https://www.stimson.org/2025/assessing-cyber-risks-and-resilience-in-india-and-pakistan/

14 Supra Note 14

15 Haridas, G., Sohee, S. K., & Brahmecha, A. (2025). *The key policy frameworks governing AI in India*. Access Partnership. https://accesspartnership.com/opinion/the-key-policy-frameworks-governing-ai-in-india/

16 Rana, A., Agrawal, S., & Bhatia, A. (2025, July 29). *CERT-In's new BOM guidelines: What India's software, AI, and hardware ecosystem needs to know*. AZB & Partners. https://www.azbpartners.com/bank/cert-ins-new-bom-guidelines-what-indias-software-ai-and-hardware-ecosystem-needs-to-know/

17 Supra Note 11

18 Supra Note 14

19 Sadeh, R. (2025, July 15). *The trust gap in AI-powered security: Why explainability matters more than ever*. The AI Journal. https://aijourn.com/the-trust-gap-in-ai-powered-security-why-explainability-matters-more-than-ever/

20 Ayndri. (2024, December 23). *Deepfake cyber threats to the financial sector in India: A growing concern*. CyberPeace. https://www.cyberpeace.org/resources/blogs/deepfake-cyber-threats-to-the-financial-sector-in-india-a-growing-concern

CHAPTER 8

AI and the Risk Spectrum: Misinformation, Hallucinations, Bias and Privacy

Introduction

In June 2025, the Air India flight crash exposed a darker dimension of generative AI (gen AI). Within hours, fabricated images and videos of victims spread online, blurring truth and fiction and even misleading experts.[1] This stark incident illustrates how AI can be used to weaponise real events, fabricating believable but false content that misdirects public understanding. This episode is not an isolated aberration but a preview of the broader societal disruptions emerging alongside rapid AI diffusion. As these tools become more accessible, their misuse scales just as quickly, colliding with India's evolving digital ecosystem.

NITI Aayog's AI strategy highlights healthcare, agriculture, education, smart cities, and mobility as high-impact areas for AI-driven growth, and reports project that AI could add up to US$500–600bn to India's economy by 2035.[2] ChatGPT usage in India recently jumped fourfold in one year,[3] but it has also brought an increased focus on issues like accuracy, bias, and privacy. India's context makes these risks especially acute. Over half of India's internet users live in rural areas, many with limited digital literacy. This demographic has become highly vulnerable to online harms. A 2024 Digital Deception report found deepfake-related cybercrimes in India up 550 percent since 2019 (including fake e-KYC and scam apps).[4]

Two structural risk vectors magnify these individual incidents into systemic threats. The first challenge lies in market concentration. AI development requires enormous computational resources, data access, and technical expertise. The structural market conditions favour a handful of large global firms. This concentration risks algorithmic dependency where domestic startups and public institutions rely on foreign models, stifling local innovation and undermining digital sovereignty.

This chapter has been contributed by Krishaank Jugiani, Senior Research Associate, CUTS International

Even within India, unequal access to computing and data can produce monopolistic tendencies towards bigger firms, marginalising smaller or vernacular AI ventures. Such dominance complicates competition policy, as conventional antitrust tools are ill-suited to data-driven, rapidly evolving AI markets, and these structural imbalances ultimately heighten societal risks by concentrating power, limiting accountability, and deepening existing inequalities.

Regulatory frameworks face a parallel issue. Existing laws like the Information Technology Act, 2000 and sectoral rules may not be fully equipped to handle the layered harms of misinformation, bias, privacy breaches,[5] including when these occur simultaneously. This may also create jurisdictional overlaps and enforcement gaps.

Regulators must therefore balance innovation incentives with accountability through mechanisms like algorithmic audits, explainability standards, and interoperable data norms without deterring growth. Additionally, India's linguistic and demographic diversity demands context-specific rules that encourage open, transparent AI ecosystems. These two vectors—market structure and regulatory design—combine with India's social realities (linguistic diversity, uneven literacy, state use of technology) to shape where and how AI harms occur.

India's Structural Realities Shaping AI Harms

In India's diverse socio-economic context, AI misuse can spread misinformation, manipulate elections, or impersonate individuals. Users may even face accidental data leaks and algorithmic manipulation as serious threats from AI platforms.[6] Most AI tools perform best in English or a few dominant languages, leaving others behind. A Johns Hopkins study shows popular large language models (LLMs) prefer information in the language of the question, and if no content exists in a low resource language, they simply default to English sources.[7]

Research has also shown that LLMs exhibit strong caste- and religion-based biases in the Indian context.[8] This suggests that AI systems can produce harmful, biased outputs. In practice, this can cocoon people of disadvantaged socioeconomic backgrounds in biased information bubbles. For instance, speakers of low resource languages face a growing divide in the availability of high quality language models and the resources required to develop them, leaving them effectively left behind and excluded.[9]

Such biases can cause informational exclusion in India. An innocuous narrative generated in Hindi may unwittingly exclude a tribal dialect (structural harm) if the model has limited exposure. Over time, this can erase local

knowledge and perspectives. Similarly, an LLM trained on biased news articles (training data risk) may both hallucinate false information (epistemic harm) and reflect social prejudices (distributive harm) in a single answer.

Further, only about 24.7 percent of Indians are computer literate,[10] and some studies suggest digital literacy at 38 percent.[11] Groups such as rural communities, women, and scheduled caste & tribe populations are especially digitally disadvantaged, both in terms of being connected and digital literacy. This creates a deep gap where AI-related harms like viral rumours, fake videos, or election misinformation can spread quickly in areas with low literacy, while many people still lack access to the tools or training needed to understand or challenge them.

Labelling synthetic media can help, but it works only if users know how to interpret those labels, and many do not. In fact, when some content is labelled, people may wrongly assume that anything unlabelled is true, a pattern known as the implied truth effect.[12] Because many users struggle to judge the credibility of online information, they are highly vulnerable to AI-generated misinformation.

India's information landscape makes AI hallucinations[13] particularly risky. Many people in India now treat AI tools as reliable information sources, with almost 20 percent saying they use chatbots weekly to stay updated on the news.[14] However, when an LLM hallucinates and confidently gives false facts, wrong laws, or incorrect medical guidance, users may accept it as true.[15] The situation may be compounded in rural or low-literacy settings. This can deepen existing knowledge gaps. Without strong digital literacy and easily accessible verification channels, hallucinations can mislead entire communities. Over time, this can erode trust in institutions, reinforce misinformation cycles, and widen the divide between those who can cross-check information and those who cannot.

Privacy risks may also play out unevenly across India's social structure. Large-scale public databases such as public welfare records often involve details of citizens. Those who are from weaker socio-economic backgrounds have little awareness or control over how their data is collected or used.[16] When AI systems trained on these datasets face cyber threats, they may be prone to leaking sensitive information or profiling. The people most affected are those least equipped to protect themselves. Marginalised groups, such as informal workers or low-income households, may be exposed to excessive surveillance through AI-powered welfare systems or policing tools.[17]

At the same time, digital literacy gaps mean many users may not fully understand nuances of consent, privacy settings, or how their data travels through AI models. This could lead to a situation in which digitally savvy

users are more likely to access the benefits of AI services, while those with limited digital agency may experience greater privacy harms such as data misuse, profiling, and surveillance, though neither group is entirely immune to either outcome.

Competition Perspective on Societal Risks of AI in India

While the market dynamics of concentration and entry barriers are central to a competition analysis, it is crucial to understand how these dynamics impact the societal risks of AI in the Indian context. The AI market exhibits a highly concentrated structure that can reinforce existing societal inequities. The recently released Competition Commission of India Market Study on Artificial Intelligence and Competition talks about the control over upstream layers of the AI stack, particularly data, computing infrastructure, and foundational models.[18]

The situation provides a significant strategic advantage to a handful of dominant players. Global big players such as AWS, Microsoft Azure, Google Cloud, and NVIDIA dominate these critical inputs, while approximately 67 percent of Indian firms operate only at the application layer and a mere 3 percent are engaged in foundational model development.[19] This market concentration directly impacts how AI harms manifest across Indian society.

When AI development is controlled by a few entities with homogeneous training data and algorithmic approaches, the systems tend to perform poorly for marginalised groups and regional language speakers. The CCI study found that 76 percent of Indian startups rely on open-source AI tools, while 43 percent use hybrid architectures combining proprietary and open systems. However, this reliance does not eliminate the fundamental power imbalances. Rather, it creates a dependency dynamic where smaller firms must align with the technical standards and business practices of dominant platforms, potentially perpetuating the very biases and exclusions discussed in previous sections.

Dominance by a handful of global tech firms has created an AI ecosystem in which foundational models largely reflect English-language and Western viewpoints, leading to a persistent and systemic underrepresentation of local and regional linguistic and cultural diversity.[20] As these models become embedded in Indian apps and services, their initial biases get scaled across the digital economy, leaving millions of users, including farmers, students, and workers, receiving inaccurate or culturally irrelevant outputs.

For instance, Khandelwal et al (2024) found that most leading LLMs systematically reinforce Indian religious and caste stereotypes, often more

strongly than US-centric biases, driven by skewed training data, a Silicon Valley-centric development pipeline, and frequency imbalances such as "Brahmin" appearing far more often than "Dalit," highlighting how global models can structurally misrepresent marginalised Indian communities.[21] With few genuinely India-centric competitors, there is little market pressure to correct these flaws, causing algorithmic exclusion to become a structural feature rather than a technical accident.

This concentration of power within generative-AI ecosystems amplifies the risk of AI-driven misinformation in profound ways. Engagement-driven models reward content that garners attention, regardless of its truthfulness. Gen-AI makes it trivially cheap and fast to mass-produce persuasive, deeply personalised synthetic narratives which, in a politically sensitive, multilingual society like India, can distort public opinion at scale.

The rapid rise of synthetic media (video, audio, images, and text) now threatens trust, identity, and social cohesion. Because platforms lack strong, contextualised content-verification mechanisms, harmful content can spread unchecked. The detection tools, like watermarking and metadata tracking, are inherently imperfect and face an arms race with malicious actors, producing errors (false positives and negatives) that can undermine public trust.[22] Embedding provenance markers also raises serious privacy risks. Watermarking or metadata tagging may inadvertently expose sensitive identities, especially for vulnerable users who rely on anonymity. In the absence of meaningful alternatives or competition, platforms lack strong incentives to deploy rigorous safeguards.

India's Legal and Institutional Fit: Existing Laws and Gaps

In the absence of a dedicated AI law, India regulates AI, especially synthetic media, through a mix of existing statutes, guidelines, and recently proposed rule changes. In practice, this means that India's AI governance relies on multiple overlapping legal anchors, each addressing only parts of the lifecycle of AI systems. Core instruments such as the Digital Personal Data Protection (DPDP) Act, 2023, sectoral regulations, and the IT Rules provide fragments of oversight, while new proposals like the 2025 synthetic-media amendments attempt to retrofit older laws to emerging risks.

This piecemeal framework draws on legacy digital governance frameworks such as the IT Act but is now being stretched to address novel harms posed by generative AI, deepfakes, and other synthetic content. The result is an evolving but uneven regulatory architecture, where some harms (for example, deepfakes, data misuse) are addressed more directly than others (for example, algorithmic discrimination, autonomous decision-making, model accountability).

A key recent development within this evolving framework is the draft amendment to the IT Rules released in October 2025,[23] which marks one of the first explicit attempts to regulate synthetic media in India. The proposed amendments introduce new compliance requirements, including mandatory visible or audible labelling on at least 10 percent of the screen area or initial audio duration of synthetically generated content, the embedding of permanent unique identifiers or metadata, and verification of user declarations by significant social media intermediaries through technical measures. However, the draft has attracted criticism from stakeholders, who argue that the definition of synthetic content is overly broad, that the requirements are technically difficult to implement at scale,[24] and that existing provisions of the IT Act, such as Section 66D, already address harmful cases of deepfakes.[25] The table below summarises the main components of this fragmented landscape and how they apply, or fail to apply, to modern AI and synthetic media.

India's broader approach to AI regulation can be characterised as techno-legal and largely principle-based, emphasising compliance, rather than ex ante regulation. There is no statutory requirement for mandatory fairness audits, dataset documentation, model transparency, or pre-deployment impact assessments for high-risk AI systems, leaving biased and opaque systems unchecked in both public and private deployments, and enabling discriminatory outcomes.

Scholars and policy analysts have repeatedly noted the absence of binding algorithmic-accountability mandates in India's current legal architecture.[27] The regulatory posture remains largely reactive rather than preventive. For instance, the obligations under draft amendments to the IT Rules depend on compliance by intermediaries and broad duties rather than enforceable detection, benchmark standards, or mechanisms to prevent harmful content before it spreads. Such reactive, platform-burdened controls are inconsistent and slow, leaving room for misinformation to proliferate ahead of enforcement.

The DPDP Act and accompanying Rules address general data protection and privacy, but do not extend to algorithmic accountability or detailed impact reporting, creating fundamental transparency and audit gaps in governance.[28] The Act, while establishing a baseline for personal data protection, remains technology-neutral but lacking in AI-specific safeguards. For instance, it does not mandate explainability, bias mitigation, or comprehensive redress for harms arising from automated decision-making processes.[29] Without clear rules for algorithmic profiling or obligatory impact assessments, decisions derived from opaque AI models can go unchallenged, disproportionately affecting marginalised populations.[30]

Overview of India's Regulations impacting AI

Regulation / Initiative	Primary Focus	How It Applies (or Will Apply) to AI/Synthetic Media	Gaps, Risks & Challenges
Information Technology Act, 2000 (IT Act)	Cybergovernance, intermediary liability	Criminalises impersonation (Section 66D), privacy violations (66E), obscene deepfakes (67A/67B), and allows blocking (69A). Safe harbour (79) tied to due diligence.	Not AI-specific; reactive enforcement; no duties for AI detection/labelling; attribution problems.
Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021 (IT Rules, 2021)	Platform duties, user harm prevention	Prevent dissemination of deceptive, privacy-violating or child-harmful content. Remove morphed/ impersonation content exposing private areas / full or partial nudity / sexual acts / impersonation (including artificially morphed images) content within 24 hours of complaint.	Reactive model; relies on user reporting; no proactive AI detection mandates.
Proposed 2025 amendments to Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021[26]	Regulation of synthetic / AI-generated content and expansion of intermediary due-diligence obligations	Introduces a formal definition of "synthetically generated information" (i.e. AI-created/modified content). Requires mandatory labelling of AI-generated content (for example, at least 10 percent of screen or initial audio), metadata, traceability, and enhanced platform due diligence obligations.	Risk of over-censorship; metadata challenges; privacy concerns; burden on smaller platforms; unclear enforcement
Digital Personal Data Protection (DPDP) Act, 2023	Regulation of personal data that includes collection, processing, and consent	Governs data used for AI training; rights of access/correction/erasure; obligations for protecting personal data processed by AI.	No automated-decision safeguards; unclear rules on synthetic data; broad "legitimate purpose"; board capacity concerns.
Bharatiya Nyaya Sanhita (BNS), 2023	Cheating, defamation, obscenity	Covers AI-generated impersonation, forged documents, defamatory deepfakes, obscene synthetic content.	Laws were built for human-led crimes; unclear liability when AI autonomously produces harmful content.
MeitY Advisories (2023–24)	Deepfake warnings, platform obligations	Require platforms to warn users, label synthetic content, and curb election-related deepfakes	Legally non-binding; earlier stricter norms rolled back; implementation inconsistent.
MeitY/IndiaAI Governance Subcommittee (AI Guidelines)	Voluntary governance principles for AI	Proposes a lifecycle approach to AI risk, from data provision '! model building '! deployment '! use.	Non-binding; no liability structure or audit requirements; weak redressal mechanisms.

Another concern of AI harms is the state processing exemptions and weak oversight mechanisms in current laws, which allow large-scale surveillance and AI-enhanced profiling with limited transparency or independent audit trails. For example, Telangana's expansive deployment of facial-recognition and biometric systems, including recent tenders for automated multimodal biometric identification, and the ensuing legal challenge in the Telangana High Court illustrate how state procurement and operationalisation of surveillance technologies can proceed with minimal statutory oversight.[31] This compounds risks to civil liberties and privacy, especially in contexts where AI systems make automated inferences about individuals without robust accountability requirements.[32]

While binding legal mandates for AI governance are largely absent, India has developed a suite of institutional guidelines and initiatives recommending increased transparency and governance mechanisms across the AI value chain. The India AI Governance Guidelines (2025) lay out a principle-based framework that situates regulators such as the Reserve Bank of India (RBI), Securities and Exchange Board of India (SEBI), Telecom Regulatory Authority of India (TRAI), and others within a coordinated governance architecture, emphasising ethical and risk-informed oversight without prescribing enforceable legal mandates.[33]

At the same time, the government has pursued strategic public investment in AI capability through initiatives such as the IndiaAI Mission, which aims to expand domestic compute infrastructure, datasets, and research capabilities to narrow the AI divide and foster innovation. This reflects a policy strategy that seeks to balance digital competitiveness with governance concerns, but also underscores the challenge of coupling investment with robust safeguards.[34]

Despite this techno-legal emphasis and strategic support for AI capacity building, significant regulatory gaps remain: clear mandates for explainability, model documentation, algorithmic impact assessments, liability for AI errors or hallucinations, and enforcement capacity are absent or underdeveloped. Without a dedicated harmonised AI regulatory framework, the current reliance on overlapping statutes and voluntary principles leaves structural issues such as algorithmic bias, misinformation propagation, privacy incursions, and unclear liability only partially addressed, and digitally disadvantaged populations are especially vulnerable as a result.

Effective policy design should combine clear, narrow ex-ante safeguards for high-risk AI applications, for example., mandatory audits, impact assessments, explainability duties, and baseline performance benchmarks. This should be coupled with light-touch support such as regulatory sandboxes, templates, and compliance assistance for innovators, drawing on global frameworks while ensuring contextual suitability and enforceability.[35]

Addressing Risks: Technical, Regulatory and Ethical Tools

Effective AI governance requires multiple layers of safeguards. Technical controls can help prevent or catch problems before deployment, while regulatory and market measures provide external guardrails. Other necessary components are model documentation (model cards, datasheets), adversarial testing and red-teaming, provenance and watermarking, privacy-preserving training, continuous logging and human-in-the-loop reviews, impact assessments, incident reporting, certification regimes and competition remedies. Together, they form the layered controls that can prevent or contain many common failure modes of generative and decision-support systems. The U.S. National Institute of Standards and Technology (NIST) has likewise emphasised internal and external evaluation, red-teaming and lifecycle monitoring as core risk-management practices for generative AI.[36]

But technical measures require adjacent legal and evidentiary scaffolding to be effective. Watermarking, metadata and provenance are only as valuable as the standards that define their format, robustness, and admissibility. Without specification of detection thresholds, accepted watermarking protocols, and preserving metadata, provenance signals will be partial and contestable in practice. The EU's AI framework signals this point by coupling content-labelling duties with explicit technical obligations and documentation, thereby making provenance an enforceable trace rather than merely a recommendation.[37]

Further, verification requires quantitative performance criteria and accredited testbeds. Red-teaming and adversarial testing are essential, but governance must answer the question "how good is good enough?" that is, define acceptable false-positive and false-negative rates for detectors, minimum coverage for fairness audits, and standards for robustness tests. Absent benchmarked performance criteria and a registry of accredited third-party verifiers, certification risks are performative rather than preventive.[38] NIST and other standard-setting bodies emphasise evaluation but leave the normative thresholds to policy choices.[39] India must convert those choices into calibrated pass/fail criteria for high-risk uses.

Human factors and the last-mile problem require explicit policy complements. Labelling synthetic media is valuable, but psychological studies demonstrate the implied-truth effect. Attaching warnings to a subset of false content can increase perceived accuracy of unlabelled items among users who lack the skills to interpret labels (a real risk in low-literacy settings).[40] In India, where household digital literacy is limited and access uneven, labels alone will protect the digitally fluent while leaving many exposed. Effective labelling, therefore, requires simultaneous investment in user education, UI design for low-bandwidth and multilingual contexts, and targeted public campaigns.

Incident reporting must also be operationalised with law defining the trigger conditions that constitute a reportable incident, setting timeframes for disclosure to the regulator and affected persons, and establishing protocols for confidential versus public disclosures and regulator intervention. The EU model offers useful reference points, but operational rules must be specified ex ante to avoid ad hoc enforcement.[41]

Finally, market and competition remedies should be concrete and staged. Mandates for data portability and API access are valuable in principle, but they require sector-specific syntaxes, pilot interoperability projects and immediate public compute and dataset investments so that smaller firms can meaningfully compete.[42] Early, low-cost interventions, including open compute grants, public datasets for low-resource languages, and accredited audit labs, can lower compliance costs and reduce the risk that regulation simply privileges incumbents.

Recommendations

Rather than adopting a single external regulatory model, a pragmatic hybrid approach is recommended. This approach should be grounded in domestic realities such as multilingual data ecosystems, uneven levels of digital literacy, a large SME base, and public-private partnerships for AI systems. Three recommendations emerge as particularly salient.

First, the regulatory framework should clearly delineate unacceptable and high-risk AI uses and impose pre-deployment obligations for a narrowly defined set of public-impact applications. A risk-based taxonomy can help identify a limited core of critical-risk systems such as welfare eligibility determination, biometric identification in public spaces, credit scoring, and certain forms of automated policing. These risks warrant ex-ante requirements, including impact assessments, documentation, human oversight, and system logging.

However, the scope of such obligations should be based on the firm's size to avoid imposing disproportionate compliance burdens on startups and small enterprises. To prevent regulatory capture by large incumbents, these requirements should be accompanied by structured compliance support, including standardised templates, regulatory sandboxes, and subsidised verification mechanisms.

Second, a strong central coordinating function is needed to ensure coherence while preserving regulatory agility. A dedicated coordination body can play a critical role in issuing iterative technical guidance, maintaining model documentation standards, operating national sandboxes, and mobilising research capacity. Such a body should also align sectoral regulators on

shared technical norms and maintain transparency through mechanisms such as a public registry of government AI deployments. Coordination should not substitute for binding obligations, rather, it should enable faster standard-setting, reduce fragmentation, and ensure that enforcement actions are informed by evolving technical expertise.

Third, regulatory obligations should be paired with industrial support and phased compliance pathways. Targeted requirements for critical-risk systems, such as certification or independent audits, are more likely to succeed when coupled with public investment in enabling infrastructure. This includes subsidised access to computing, accredited testing and audit facilities, workforce development programmes, and accelerated certification tracks for early-stage firms. Strategic investment in multilingual datasets and open foundation models can further reduce dependence on large incumbents and lower compliance costs for domestic innovators, ensuring that regulation supports, rather than constrains, the development of a competitive AI ecosystem.

Conclusion

The rapid diffusion of generative AI in India is unfolding against a backdrop of deep social diversity, uneven digital literacy, concentrated market power, and fragmented regulation. As the Air India crash incident illustrated, the harms enabled by generative AI are no longer speculative or abstract, rather immediate, scalable, and capable of distorting truth, trust, and accountability within hours. What distinguishes the Indian context is not merely the presence of these risks, but the way structural inequalities amplify them.

Linguistic marginalisation, socio-economic vulnerability, and asymmetries in access to digital skills mean that the costs of AI failure are borne disproportionately by those least equipped to contest or correct them. Bias, misinformation, hallucinations, privacy intrusions, and surveillance are not isolated technical defects but systemic outcomes shaped by training data, platform incentives, and regulatory gaps. Market concentration in foundational models and compute infrastructure further entrenches these risks by limiting diversity in design choices and weakening competitive pressure to correct harmful outcomes.

In parallel, India's current legal and governance framework reflects a transitional moment. While existing statutes such as the IT Act, DPDP Act, and sectoral laws provide partial remedies, they were not designed for autonomous, generative, and probabilistic systems that blur authorship and responsibility. The emerging approach, which includes retrofitting older laws through advisories and draft amendments, has helped signal intent but

remains largely reactive, fragmented, and dependent on platform compliance. Crucially, binding obligations for algorithmic accountability, pre-deployment risk assessment, and clear liability allocation remain absent. In such a setting, harms are often addressed only after they have already spread, eroding public trust and compounding social damage.

At the same time, the regulation cannot rely on restriction alone. India's ambition to leverage AI for development, productivity, and public service delivery is legitimate and necessary. The challenge lies in aligning this ambition with safeguards that reflect domestic realities: multilingualism, low digital literacy, a large SME ecosystem, and state use of AI. Effective responses, therefore, require a layered approach that combines technical risk controls, calibrated legal duties, competition remedies, and sustained public investment in capacity-building. Without parallel investments in compute access, local datasets, auditing infrastructure, and digital literacy, even well-designed regulation risks entrenching incumbent power and excluding smaller innovators.

Ultimately, the societal risks of generative AI in India are inseparable from questions of institutional design and distributive justice. How AI systems are built, who controls them, how they are deployed, and who is protected when they fail will shape whether AI deepens existing inequalities or contributes to more inclusive growth. Addressing these risks demands moving beyond ad hoc responses toward a coherent, risk-based governance framework that is preventive rather than merely remedial. In doing so, India has the opportunity not only to mitigate harm, but move towards developing an AI regulation approach—one that foregrounds social context, democratic accountability, and equitable access in an era of accelerating technological change.

Endnotes

1 https://incidentdatabase.ai/cite/1125/

2 https://niti.gov.in/sites/default/files/2025-09/AI-for-Viksit-Bharat-the-opportunity-for-accelerated-economic-growth.pdf

3 https://economictimes.indiatimes.com/tech/technology/ashwini-vaishnaw-openais-india-entry-will-power-inclusive-ai-under-indiaai-mission/articleshow/123465825.cms?from=mdr

4 https://waccglobal.org/deepfakes-cloned-voices-and-digital-media-literacy-ais-role-in-the-misinformation-crisis-in-india/

5 https://arxiv.org/pdf/2509.09508

6 https://timesofindia.indiatimes.com/city/pune/sharing-personal-data-on-ai-carries-risk-of-leak-to-dark-web-warn-experts/articleshow/125116363.cms

7 https://hub.jhu.edu/2025/09/02/multilingual-artificial-intelligence-often-reinforces-bias/

8 https://arxiv.org/pdf/2309.08573

9 https://cohere.com/research/papers/the-ai-language-gap.pdf

10 https://www.thehindu.com/opinion/lead/computer-literacy-in-india-needs-a-reboot/article68367762

11 https://www.ideasforindia.in/topics/governance/the-digital-dream-upskilling-india-for-the-future.html

12 https://cuts-ccier.org/pdf/reimagining-content-moderation-strategies-in-the-age-of-generative-ai.pdf

13 AI hallucination occurs when AI models, especially large language models (LLMs), generate plausible but factually incorrect, fabricated, or nonsensical outputs presented as truthful.

14 https://www.thehindu.com/news/national/indians-turning-to-artificial-intelligence-for-news-influencers-find-big-audience-report/article69700348.ece

15 https://www.medianama.com/2025/03/223-justice-gavai-flags-ai-risks-when-chatgpt-gets-legal-facts-wrong/

16 https://www.ijllr.com/post/the-aadhaar-paradox-privacy-vulnerabilities-and-marginalization-in-india-s-aadhaar-system

17 https://ohrh.law.ox.ac.uk/ai-surveillance-and-privacy-in-india-human-rights-in-the-age-of-technology/

18 https://www.cci.gov.in/images/marketstudie/en/market-study-on-artificial-intelligence-and-competition1759752172.pdf

19 https://www.cci.gov.in/images/marketstudie/en/market-study-on-artificial-intelligence-and-competition1759752172.pdf

20 https://arxiv.org/html/2412.04774v1

21 https://arxiv.org/pdf/2309.08573

22 https://cuts-ccier.org/pdf/reimagining-content-moderation-strategies-in-the-age-of-generative-ai.pdf

23 https://www.meity.gov.in/static/uploads/2025/10/708f6a344c74249c2e1bbb6890342f80.pdf

24 https://economictimes.indiatimes.com/tech/artificial-intelligence/tech-groups-flag-implementation-challenges-with-proposed-ai-rules/articleshow/125305839.cms

25 https://inc42.com/buzz/iamai-raises-red-flags-on-meitys-draft-ai-labelling-rules/

26 Draft/consultation (subject to change)

27 https://www.defindia.org/wp-content/uploads/2025/03/DCS-Report-2025_24-Jan-2025_.pdf

28 https://defactolawjournal.org/papers/why-we-need-data-protection-laws-for-ai-in-india/

29 https://ijirl.com/wp-content/uploads/2025/06/ISSUES-AND-CHALLENGES-IN-THE-PROTECTION-OF-RIGHT-TO-PRIVACY-IN-THE-ERA-OF-ARTIFICIAL-INTELLIGENCE-AN-OVERVIEW.pdf

30 https://iisppr.org.in/ai-and-data-protection-challenges-in-automated-decision-making-2/

31 https://www.medianama.com/2024/03/223-telangana-police-tender-biometric-identification-system/

32 https://futurefreespeech.org/wp-content/uploads/2025/10/AI-Report-India.pdf

33 https://indiaai.s3.ap-south-1.amazonaws.com/docs/guidelines-governance.pdf

34 https://hai.stanford.edu/assets/files/hai_ai-index-report-2025_chapter6_final.pdf

35 https://iapp.org/resources/article/global-ai-governance-india

36 https://nvlpubs.nist.gov/nistpubs/ai/NIST.AI.600-1.pdf

37 https://www.europarl.europa.eu/RegData/etudes/BRIE/2023/757583/EPRS_BRI percent282023 percent29757583_EN.pdf

38 https://hai.stanford.edu/assets/files/hai-policy-brief-what-makes-a-good-ai-benchmark.pdf

39 https://airc.nist.gov/airmf-resources/airmf/5-sec-core/

40 https://pubsonline.informs.org/doi/10.1287/mnsc.2019.3478

41 https://www.europarl.europa.eu/RegData/etudes/BRIE/2023/757583/EPRS_BRI percent282023 percent29757583_EN.pdf

42 https://www.oecd.org/content/dam/oecd/en/publications/reports/2021/10/data-portability-interoperability-and-competition_f09a402e/73a083a9-en.pdf

CHAPTER 9

The AI Workforce Equation: Skilling for a Transforming Economy

Introduction

Artificial intelligence (AI), a new global benchmark for digital technologies, is rapidly being recognised as a key force behind economic development and increased labour productivity in many industries. With the huge adoption of AI, there is a rise in the need to upskill or reskill the professional profile of employees to adapt to the new job requirements. The conversation around AI is usually positive, ignoring the basic problem, which is the unequal access to AI-related skill development opportunities across various regions of India. The human factor is a severe constraint to AI integration, as a huge number of workers lack advanced digital skills that enable active interaction with AI.

The purpose of this study is to analyse the widening gaps in AI education and skill development across India's Tier 1, Tier 2, and Tier 3 cities and urban and rural areas and how the gap leads to the underutilisation of human resources.

India took multiple steps towards digital transformation and skill enhancement; however, urban biases still exist. The majority of private EdTech platforms and AI skilling initiatives are found in Tier 1 universities like IITs, leaving out the students and young professionals in smaller cities and towns. It is not because the students of the smaller towns are incapable of gaining these skills, but because of a lack of knowledge, infrastructure limitations, regional training programmes, and policy drawbacks. There exists misallocation of human capital where a significant portion of India's potential AI workforce remains unemployed. This affects the labour market outcomes and increases the regional disparity over time.

This chapter has been contributed by Divya Aggarwal, Research Associate at Office of Gopal Krishna Agarwal.

To evaluate the geographical differences in access to AI skills, a mixed-method approach is followed in the study, combining primary research with secondary data. To conduct primary research, an online survey was created and distributed to students and young professionals in various parts of India. The data on awareness levels, perceived hurdles to participation, availability of digital infrastructure, and access to AI skilling possibilities were gathered through the survey.

After a thorough analysis, the paper details the policy recommendations based on inclusive human capital development and labor market efficiency to solve the inequality issues. The recommendations detail suggestions on national and state-level skilling programmes, following a region-specific allocation. The study will further discuss the need for regulatory bodies like the National Skill Development Corporation to make it compulsory for private skill providers to operate in underprivileged areas and how public-private partnerships can be utilised to create AI skilling content in regional languages. Skilling platforms must follow data transparency to reveal participation and placement results by region.

The study argues the importance of resolving disparity in AI skills for economic competitiveness. As the country aims to become a global powerhouse for AI, a large segment of India's population cannot be left behind in the AI revolution. There will be the realisation of the entire human capital potential of the country when workers in rural and small towns, as well as students, have equal access to AI-driven economic transformation.

The report highlights the need to reduce regional gaps in AI skills from an economic viewpoint. Therefore, it provides practical insights into the changing skilling policy landscape of India and prevents an argument for incorporating regional inclusion into India's AI skilling regulatory framework.

Overview of AI's Transformative Role in the Global and Indian Economies

The rapid advancement of artificial intelligence (AI) has caused both excitement and concerns in economies across the globe. There have been multiple questions around how AI would impact the global economy, mainly involving the discussions on its impact on the labour market and whether jobs will be replaced by AI.

According to the reports, AI is expected to contribute US$13tn to the global economy by 2030 (Jiang et al., 2025). This change would be marked by labour substitution, innovation in products and services, and new AI-related jobs. By 2028, AI and automation are expected to create 69 million new job roles in sectors such as data analysis, machine learning, and AI development, highlighting the need for economies to focus on upskilling and reskilling programmes (Jiang et al., 2025).

With the potential to add US$500bn to the Indian economy, AI would positively affect key sectors such as agriculture, manufacturing, healthcare, and urban planning (Kaushik et al., 2025). However, with this change, India needs to not only focus on advanced technology but also on the equitable access of resources to individuals.

The Ministry of Electronics and Information Technology of India launched the AI for India 2030 initiative to integrate AI into India's socio-economic fabric, emphasizing the ethical, responsible, and inclusive use of AI. If used strategically, it can solve the country's socio-economic challenges, such as agricultural yield, healthcare, and manufacturing efficiency. In India, a country known for its demographic diversity, it is evident to see the dual impact of AI, where it has created high-skilled employment opportunities but also led to displacement in job roles in low-skilled job sectors.

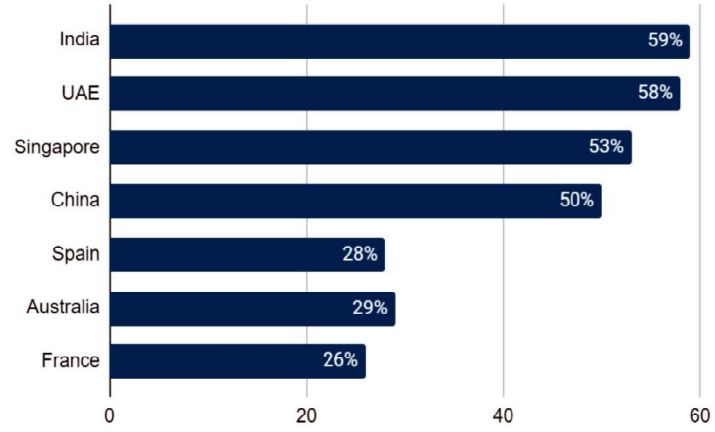
Growing Demand for AI-related Skills in the Labour Market

The demand for AI-related skills is accelerating globally beyond tech roles. The employers show a strong interest in hiring AI-skilled people, including those in the non-IT sector. They often raise wages for AI-literate employees, indicating a structural, skills-led shift in the labour market.

In 2025, the global unemployment rate stood at 4.9 percent, the lowest since 1991. The middle-income countries are experiencing a reduction in the unemployment rate, but the low-income countries have experienced a rise from 5.1 percent in 2022 to 5.3 percent by 2024 (WEF, 2025). Technological change is a major driver in reshaping jobs and the required skills, wherein the World Economic Forum's Future of Jobs 2025 survey shows 86 percent of firms expect AI and information processing technologies to transform their business by 2030. Generative AI has seen a rise in its adoption and an eightfold rise in investments across multiple sectors, with an increase in investments in physical infrastructure like servers and energy generation plants needed to support these emerging technologies.

Indian enterprises have adopted AI unusually fast. IBM's Global AI Adoption research report (2024) states that 59 percent of the Indian enterprises have deployed AI by early 2024, and the financial services companies are most likely to be using AI. According to the Naukri JobSpeak Index, the AI and machine learning (ML) roles are seeing a 42 percent year-on-year growth. However, the technology companies are seeing a shortfall in the AI talent, with only 15-20 percent of the AI-skilled workforce (ETtech, 2025). A Bain & Company report stated that the job postings for AI-skilled workers have grown by 21 percent annually since 2019, and their salaries by 11 percent. It was observed that AI-skilled freshers earn four times the standard entry-level salary (ToI, 2025).

Figure 20: Global Labour Market Trends and Technology-Driven Transformation of Work

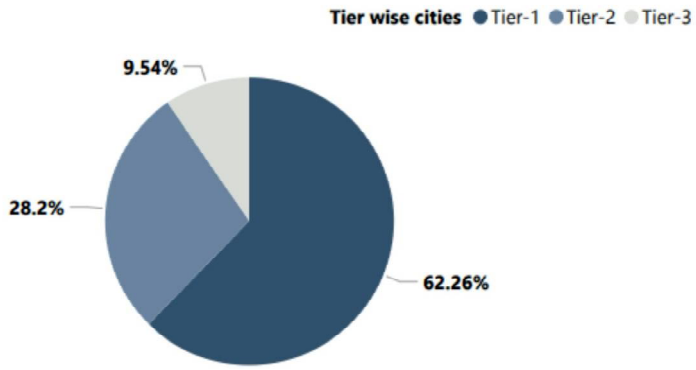


The top factors driving AI adoption are accessibility, reduced cost, automation of key processes, and an increased amount of AI embedded into standard off-the-shelf business applications. However, limited AI skills and expertise, data complexity, and ethical concerns act as barriers to the exploration and deployment of AI.

There is a widening demand for AI-related skills in India, which are not just restricted to engineering roles but combine AI literacy with domain and managerial capabilities. This encourages equitable access to AI skill development programmes across regions, and without this, the firms will face binding skill constraints, and India will underutilise a large segment of the population for its future AI workforce.

A pilot survey was conducted to analyse the regional disparities in AI access and skilling, and to identify the challenges people face. The survey gathered 461 responses, with 62.26 percent from Tier-1 cities, 28.2 percent from Tier-2, and 9.54 percent from Tier-3. This uneven spread creates a methodological concern that the averages will be skewed towards Tier-1 responses. To overcome this, the analysis emphasises within-tier patterns (percentages and mean ratings per tier) rather than pooled averages.

Figure 21: Distribution of Penetration Across Tier-1, Tier-2, and Tier-3 Cities (percent)



Statement of the problem

According to D'Monte (2025), India saw the highest year-over-year growth in AI hiring in 2024 at 33.4 percent, followed by Brazil (30.8 percent) and Saudi Arabia (28.7 percent). According to the Stanford AI Index (2024), India has a score of 2.8, making it first in AI skill penetration, ahead of the US (2.2) and Germany (1.9).

Yet AI access is uneven across India. The current studies indicate the concentration of AI-related skills and job opportunities in tier 1 and metropolitan cities of India, while the rural regions and tier 2 and tier 3 cities face persistent barriers such as affordability, infrastructure, language, and institutional outreach. This uneven concentration of opportunities has led to underutilisation of human capital outside metropolitan cities, exclusion of large sections of students and workers from AI opportunities, inefficiency in work due to mismatches between supply and demand of AI-skilled labour, and widening regional and socio-economic disparities.

Existing national skilling initiatives lack enforcement to ensure equal distribution of AI opportunities in all regions, leaving the workers concentrated in the urban areas. Without corrective measures, it would be difficult to lessen the regional socio-economic disparities in India, limiting its competitiveness in the global AI economy.

Aim

1. To identify the extent and nature of geographical gaps in AI skilling in tier 1, tier 2, and tier 3 cities, and metro and non-metro cities, focusing on level of awareness, accessibility, and perceived barriers among students and young professionals.

2. To examine the role of infrastructure, affordability, and language in shaping participation in AI skilling and training.
3. To evaluate how the regional disparities contribute to underutilisation of India's potential workforce by identifying mismatches between the availability of the AI skilling programmes and the distribution of the workforce across regions.
4. Provide well-designed policy recommendations for inclusive AI skilling and deployment to enhance human capital formation and support India's long-term economic competitiveness.

Research Questions

1. Do regional disparities in AI skilling and job roles exist? And if yes, what is the reason behind it, and how do they affect AI skilling outcomes?
2. What are the limitations of existing regulatory frameworks?
3. What policy interventions are needed to promote inclusive AI skill development?

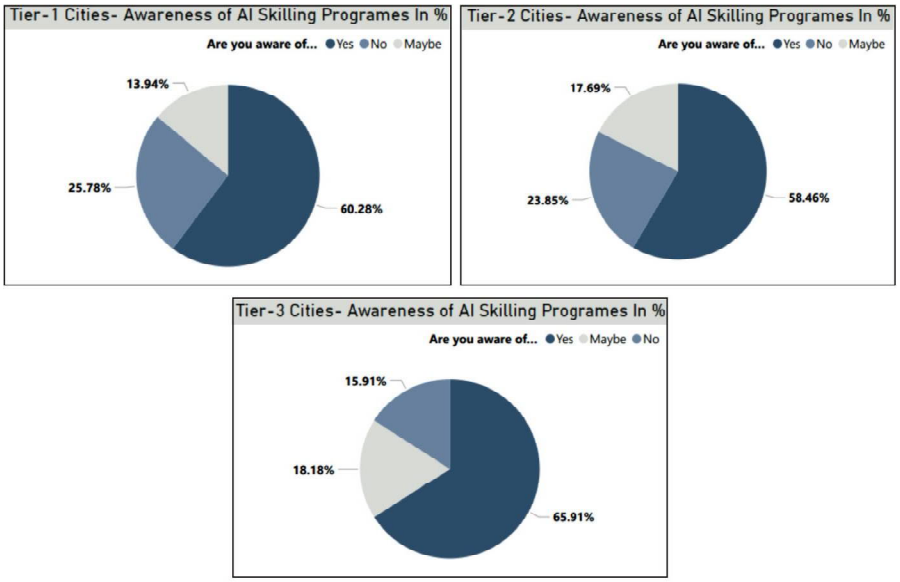
Impact of AI on the Employment

AI is rapidly transforming the Indian employment landscape, showing both opportunities and challenges. The 2025 report by Boston Consulting Group reports that 80 percent of the Indian companies consider AI as a strategic priority, even above the global average of 75 percent. Also, 69 percent of firms planned to increase their tech investments in 2025. Startup funding of Indian GenAI increased over six times quarter-on-quarter, reaching US$51mn in Q2 of FY2025. WEF (2025) reported that in 2024, 7 out of 10 employees used AI at work, showing rising integration of AI in workplaces. The government aims to create economic and employment opportunities for all Indians while also focusing on inclusive AI adoption.

Awareness level appears to be relatively even across tiers, but the gap lies in the information clarity, where tier 2 and tier 3 respondents display more hesitation, that is, the 'maybe' response. This indicates that the knowledge about AI skills and opportunities circulates less effectively beyond metros. While many respondents may have heard about AI courses, there are high chances of the understanding remaining fragmented.

Despite the rising AI adoption in India and multiple job opportunities, it still leads to job displacement, majorly in routine and manual tasks. A report released by the World Economic Forum states that by 2025, automation and AI are expected to eliminate around 5.1 million jobs in India. It would have an impact on the low-skilled workers, leading to an increase in existing inequalities in the labour market.

Figure 22: Awareness of AI Skilling Programmes in Tier 1, 2 and 3 Cities



However, the impact of AI is uneven across regions of India. Urban areas have robust digital infrastructure and access to quality education, positioning them better to use AI technologies, but the rural areas face various challenges such as financial constraints and lack of digital literacy and infrastructure, making it difficult for them to receive benefits from AI advancements.

Job displacement risks and creation potential: Sector-specific impact

The impact of AI varies across sectors. It poses a significant risk of job displacement in roles involving repetitive, manual, or routine tasks. Increasing the adoption of AI across industries will help India to grow at 8 percent, achieve its target of Viksit Bharat 2047, contribute US$500 to US$600bn to the economy, and raise productivity and efficiency of the workforce (Kaushik et al., 2025).

Manufacturing: India's manufacturing sector is labour-intensive; however, AI-driven productivity gains, predictive maintenance, and intelligent product design can add up to US$85 to US$100bn. The adoption of AI in manufacturing has helped in timely repairs to minimize downtime, detect minor defects that may go unnoticed, reduce waste, ensure high-quality output, and meet demand efficiently, while avoiding stock surplus. However, a report by McKinsey Global Institute states that 60 million workers in India's manufacturing sector are expected to be displaced by 2030 because of automation. It will highly impact the jobs in textiles and electronics.

Banking and Financial Services: AI can personalise customer experience, advance fraud detection, and make lending process more inclusive, with an expectation to add US$50 to US$55bn by 2035. There has been a fall in employment, particularly in the private-sector banks but the numbers do not reflect a widespread decline in employment in the banking sector because of AI adoption. With these new technologies, banks expect to reshape 35-50 percent of jobs (ET, 2025).

Engineering: AI has altered the landscape of the job role which was once considered the safest option. A report by Great Learning showed that 67 percent of the Indian engineers believe that AI is already reshaping their roles; however, 85 percent of the engineers felt the necessity to upskill (ToI, 2025).

Retail: AI in retail has helped companies with everything from product recommendations and pricing to inventory management and customer service. But 76 lakh jobs are expected to be affected by AI in the next five years (ET, 2025).

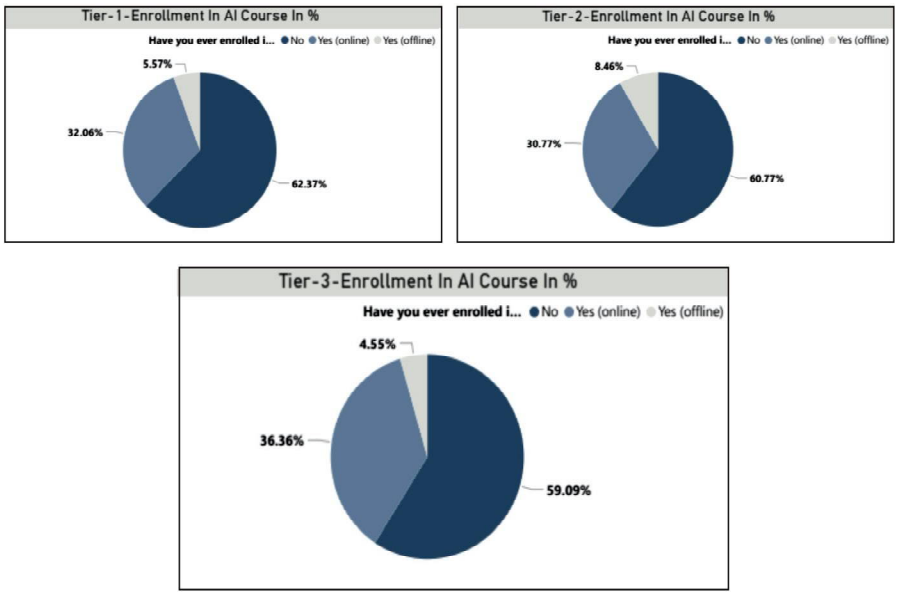
Education: AI in education raises concerns over the use of technology and loss of the traditional studying methods, like book-based learning and critical thinking. A balance between technological advancements and intellectual development is necessary for India to have a mindful generation (Godase, M., 2025). Twenty-five lakh jobs in the education sector are expected to see a significant change in the next five years. With AI having a varying impact on multiple sectors, employees are seeking job changes, mainly in the electric vehicle and engineering sector, while also expecting a 20-40 percent salary hike with AI-related skilling. India is among the top AI-adopting nations, and organisations are increasing their investments in upskilling for workforce transformation. It also allows for work flexibility, with 61 percent companies offering hybrid job roles (Basu, S., 2025).

Access to AI in tier 2 and 3 cities, and non-metro cities

According to Patra, S. (2025), AI is promising a transformative role in tier 2 and tier 3 cities. In cities like Varanasi, Indore, and Patna, AI-powered tools such as mooON wearables for cattle and smartAMCU for milk collection are used, improving productivity and enhancing farmers' income. Farmers of Varanasi have reported up to a 500 percent improvement in profitability and 160 percent higher market realisation for milk. While India has positioned itself as a global AI hub, the benefits of access of AI remain uneven. The skill divide between metro and non-metro cities, and tier 1, tier 2, and tier 3 cities, acts as a critical barrier and raises regional inequalities in access to AI-driven employment opportunities.

The AI adoption so far is concentrated in the metro-centric cities such as Mumbai, Bangalore, Delhi-NCR, and Pune. The multinational companies, global capability centres (GCCs), and large IT firms are highly present in these cities, and so is the digital workforce. Unlike these tier 1 cities, there is a lack of institutional capacity in the tier 2 and tier 3 cities. Even though there is rising awareness about AI in smaller cities, they often lack access to specialised curricula, AI labs, or mentorship from industry experts, further restricting them from the high-value jobs.

Figure 23: Tier 1, 2 and 3: Enrollment in AI Course



Enrollment levels show a significant interest of people in tier 1, tier 2, and tier 3 cities to enrol and gain AI skills. It challenges the assumption that metro cities are the only active skilling hubs. Digital platforms also help tier 2 and tier 3 learners to overcome the challenge of physical infrastructure. However, participation in offline institutes remains negligible in all the tiers, highlighting the lack of local and structured skilling institutes. The learners have to depend on self-driven models without proper supportive ecosystems.

The government, under the India AI Mission's India AI Future Skills pillar, has established 20 data and AI labs, with seven being added in tier 2 and tier 3 cities, and plans to extend these labs to 200 by March 2026 (Sharma, S., 2025). The initiative is taken to encourage inclusive development and access to AI education for all. 27 labs are identified in cities such as Gorakhpur, Lucknow, Shimla, Aurangabad, Patna, Buxar, Ropar, Haridwar, among others. Besides AI labs, efforts are being made to provide AI-related skills through EdTech platforms and virtual apprenticeships.

Setting up data labs in non-metro cities is challenging, as it includes high initial cost, lack of reliable power, land cost, logistical challenges, lack of connectivity, lack of regulatory or policy clarity, and lack of skilled personnel locally (Das & Chaliawala, 2025).

On a national level, only around 42 percent of graduates are job-ready, indicating that not even half of the graduates have advanced or AI-adjusted knowledge (ETtech, 2025). A rising use of AI and modern tools is seen in tier 2 and tier 3 cities, but it is applicable only for those who are aware of these tools and have access to devices and the internet (Roy, S., 2025).

So, these interventions for AI skilling and setting up of labs remain selective and limited in scale, whereas multiple tier 2 and tier 3 cities lack access to these labs or platforms entirely. This implies that the regions and people who are more connected or are economically better off benefit disproportionately, widening regional inequality.

Identifying the Gaps

Digital infrastructure barriers

Many rural places and small towns lack basic digital infrastructure and have a lack of reliable high-speed broadband internet, optical fibre, or fixed-line connectivity. As the mobile internet is more accessible these days, it helps them to connect, but the mobile internet is insufficient in speed, reliability, and cost that AI requires. AI deals with large datasets, streaming, or using computer-heavy tools, which the mobile internet does not support, creating difficulties in such areas. Compared to 8.4 percent urban households lacking internet access, the 16.7 percent rural households lack internet access. Even when 83.3 percent rural households have internet access, only 3.8 percent have high-speed fiber connections (Thomas, S., 2025)

Figure 24: Tier-wise Cities: Average Rating High Speed Internet, AI/Tech Members, AI Career Counselling and Physical AI Skilling Centres

Tier wise cities	Average Rating High Speed Internet
Tier-1	4.59
Tier-2	4.22
Tier-3	4.20
Total	**4.45**

Tier wise cities	Average Rating AI/Tech Mentors
Tier-1	3.31
Tier-2	2.92
Tier-3	2.73
Total	**3.15**

Tier wise cities	Average Rating AI Career Counselling
Tier-1	2.74
Tier-2	2.56
Tier-3	2.11
Total	**2.63**

Tier wise cities	Average Rating Physical AI Skilling Centres
Tier-1	2.63
Tier-2	2.38
Tier-3	2.32
Total	**2.53**

The survey included ratings on a 1 to 5 scale for infrastructure and guidance. The true disparity persists in ecosystem depth. While internet penetration has levelled up, AI mentorship, structured skilling centres, and career guidance are heavily metro-centric. Tier-3 respondents, in particular, lack exposure to experts or formal counselling, leading to isolation in their learning journeys.

According to ET (2024), the partner member of EY Global mentioned that India will require an overall investment of around Rs. 4.2 lakh crore by 2030 to connect 24 crore Indian households to broadband services. With the role of the government and CSR, the current internet penetration of 3.6 crore urban households and 30 lakh rural households is expected to reach 10 crore urban households and 15.3 crore rural households by 2030. BharatNet aims to provide broadband connectivity in rural households, but the process is taking time due to increased costs and continuous delays in Phase 3 (Parbat, K., 2024).

Even where AI-skilling programmes exist, the lack of high-speed internet creates challenges, and the students are unable to access the required content and use EdTech platforms. Also, the organisations don't wish to establish their startups in regions with low internet, due to which the lack of digital infrastructure directly impacts the skills and unemployment.

Language and content bias

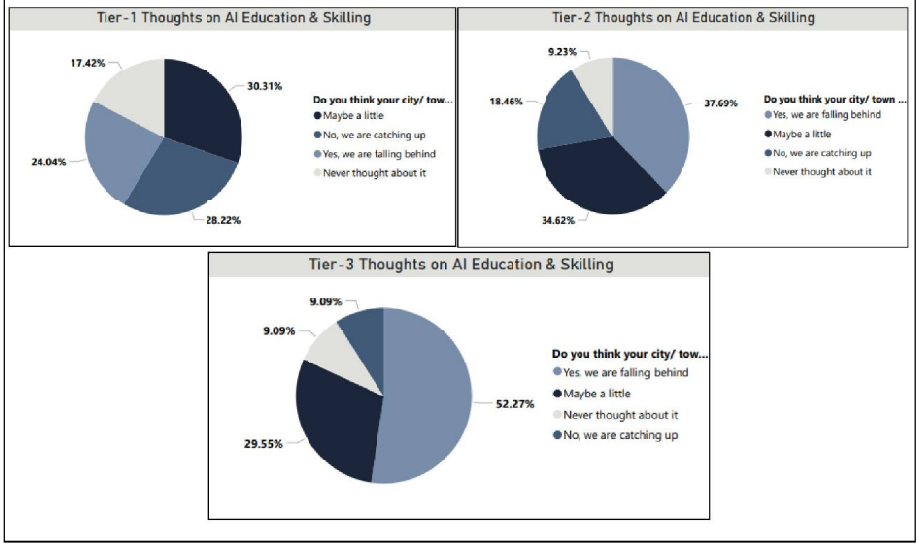
Most of the AI, ML, data science, and data analytics documentations and textbooks are primarily in English (Ghai, N., 2024). The accessibility of these courses in English makes technical terminology, assignments, and peer interaction more flexible and fluent. There are multiple course materials in regional languages or local dialects through translation, but there are

high chances of their quality being impacted (Anand, A., 2024). Also, the content delivered at this level requires some prior knowledge, like mathematics, coding, and computing environments, which might be more present in metro cities/urban areas and less in rural areas due to a lack of infrastructure.

Evidence of misallocation of human capital formation: talent exists, but not AI-ready

Many students and graduates in tier 2 or tier 3 cities have good human capital, and a few's interest also align with technology, but their training is not aligned to coding, statistics, or computing. The curriculum at many places lacks what the industry actually demands, like labs, faculty expertise, and mentorship. However, the Indian employment environment is seeing a rapid transformation where Udaipur, Vizag, Warangal, Lucknow, and Indore are emerging as job creation centres besides Bengaluru, Mumbai, Hyderabad, and Gurgaon. In cities like Coimbatore, Nagpur, and Nasik, around a 20 percent to 25 percent increase in IT service employment is observed, and around 30 percent to 40 percent in Jaipur (ET Online, 2025).

Figure 25: Tier 1, 2 and 3: Thoughts on AI Education & Skilling



About 30 percent of respondents of tier 1 believe their city is falling behind, but a comparable share feel they are catching up. Respondents from tier 2 cities have a stronger sense of lag, with around 38 percent stating they are falling behind. The respondents from tier 3 cities are the most pessimistic group, with 52 percent believing that they are falling behind, with only 9 percent feeling they are catching up. Confidence diminishes steadily from tier 1 to tier 3. Even if awareness and enrollment rates appear comparable, tier 3 respondents show the least confidence in their infrastructure capacity to support AI adoption.

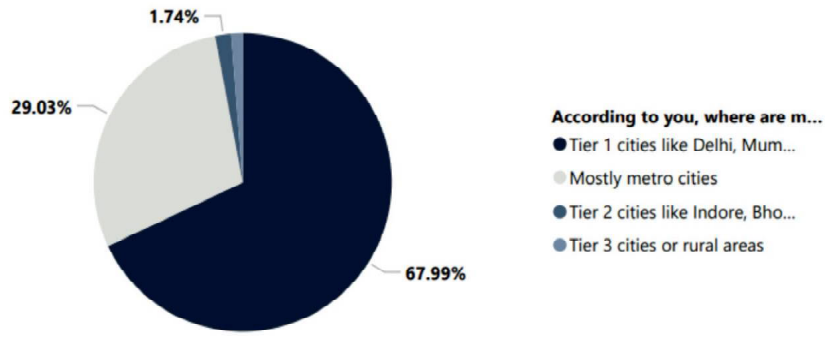
Disparities are not only about awareness but also about structured opportunities. Internet access is becoming less of a barrier, but access to mentors, skill centres, and expert counselling is widening the gap. It is believed that AI belonging to metro cities discourages learners in smaller towns from pursuing AI as a career locally, pushing talent migration. But there is a belief that if given the right support, the smaller cities and towns are capable of succeeding in an AI-driven job market.

Besides the courses, there is a need to update the curriculum of schools and universities according to industry demands. The experts are concentrated in the metro cities because of the availability of resources and higher salaries as compared to the rural areas, due to which the instructor capacity in those areas is low.

Lack of labour market mapping

The course content and the university curriculum are designed in a general manner and are not specific to what may be relevant locally, like regional health AI or local manufacturing. Currently, the students are more informed about the global dynamics and unaware of the regional situation, opportunities, or challenges.

Figure 26: AI Job Concentration



When asked about AI job concentration, approximately 68 percent pointed to tier-1 cities, while only 1.7 percent felt the availability of such opportunities in tier 3 cities. Around 29 percent believed that the jobs are concentrated in mostly metro cities, which include tier 1 cities and some tier 2 cities. The perception that real AI jobs mostly exist in metros reinforces urban migration pressures. Even if tier 2 and tier 3 learners gain skills online, they feel compelled to relocate to tier 1 cities. This perception and infrastructure gap limits local confidence in building regional AI ecosystems.

More than 50 percent of the respondents felt that AI will positively impact the current and future job prospects, but 36 percent and 37.7 percent of respondents felt that the current education is preparing us for the AI-related job roles only to some extent and not really, respectively. The biggest challenge in grabbing job opportunities in this field is a lack of skills and a lack of awareness of the job roles. However, more than 65 percent of the respondents felt that AI skills are very important for future employability. The people will be more interested in taking up the course when it is offered at a low cost, guarantees job placement or internship, and has access to online live classes.

Recently, Coursera has translated over 4,000 courses into Hindi to try to cover the regional gaps and provide course access to people who are more comfortable in Hindi (Ghai, N., 2024). This indicates the recognition of the local needs. When there is a mismatch between the curriculum and the local job demand, the employability of the region reduces, and some with the AI job potential also miss the relevant training. Also, some of the students who get trained in generic AI may not get a job locally, forcing them to migrate or remain unemployed (Godase, et al., 2025).

Gaps in current AI skilling policies

There are multiple government policies and schemes, such as IndiaAI, IndiaAI Future Skills, and skilling labs, that aim to enhance the AI skilling of the Indians, but the weak regulatory procedure does not let these policies/ schemes reach the backward regions, and there also exists a gap in transparency & accountability in public/private skilling outcomes.

The centres are preferably opened in areas that have more requirements, like those in metro cities. It is not mandated or subsidised by the government to open at least some specific number of AI-skilling centres in the backward regions.

The National Skill Development Corporation or similar bodies don't perform transparent regional reporting, like the number of students trained in specific regions and their placement in companies. The private EdTech firms operate without government intervention, which gives them the liberty to function

according to themselves, raise course costs, content quality, and language inclusion, allowing them to be more profit-oriented and operate in urban markets.

Policy Recommendations

Framing generic policies for industries overall and for specific issues does not help in resolving the issue at the level thought, but there are higher chances of rising regional disparities with it. The government and organisations need to move from a general policy-making approach to a region-specific or sector-specific approach that recognises India's socio-economic and geographic diversity. The following recommendations are designed to enhance inclusivity and a region-specific approach and ensure a long-term market approach.

1. Mandatory Backward Region AI Development

The government can take a 'backward region quota or subsidy' approach to develop AI-skilling centres and labs in tier 2 and tier 3 cities and prevent them from remaining concentrated in the metro cities or urban areas. Under this, there should be a mandatory obligation to set up well-designed AI-skilling centres, labs, or EdTech partnerships in the tier 2 and tier 3 cities. The government, besides the quota, can also provide subsidies to those organisations to allow students to take up the course at a low cost.

Based on the Human Development Index (HDI), internet penetration, and unemployment levels, the regions can be identified, and AI centres and labs can be established. Current policies focus on establishing these centres in areas with high demand, increasing regional disparities. District-level colleges or centres can host these programmes, saving the cost of setting up more new centres, further reducing the migration of those talents to the metro cities, leaving their home region's growth stagnant.

2. Development of Curriculum Localisation Hubs

A higher percentage of AI courses are available in English, creating a language barrier and excluding people who are not fluent in English from getting AI-trained. State-level hubs can be established to adapt the national AI courses to their regional languages. These hubs can get a few AI experts from their region and co-create the curriculum in the regional language, which is also relevant to local economic sectors.

These hubs can partner with the state-level body and the institutes and can propose for funding through CSR. Co-creating the course will help in better coverage of the course rather than translating it, improving local employability.

3. Encouraging Regional Data Sets and Transparency

An independent 'Regional AI Skilling Index' should be established, which would be state-wise and district-wise data. It can include rankings on performance on access, enrollment in the courses, the percentage of people who completed the courses, the dropout rates, and placement outcomes.

Anonymous regional data shall be released by Private EdTech platforms and NSDC-affiliated training institutes. A third party can be asked to compile the data and form an index. Also, data can be made available in multiple languages, rather than restricting it to English and Hindi.

The current reporting of data is opaque, creating confusion about reality, and this approach might introduce accountability and competitive benchmarking. It will further help policymakers to plan according to the lagging regions and allocate funds effectively.

4. AI Skilling Obligations for Large Employers

A regulatory requirement to be introduced for companies above a certain turnover to contribute a portion of their CSR to AI-skills training in rural areas, tier 2, tier 3, and non-metro cities. India has CSR laws but they do not yet mandate AI-related or skill CSR laws.

These policies would help private companies to explore talent in backward or left-out regions. IT firms in Hyderabad or Bengaluru can fund AI labs or scholarships in districts like Gaya, Imphal, or Kalahandi. This will ensure the circulation of the private funds for the greater good towards the areas that are usually ignored by the market, leaving them to stay reliant on the government.

5. Improving Digital Infrastructure

Instead of relying on the large telecom owners, the states should encourage community-owned digital cooperatives at the district or block level, to expand last-mile connectivity. The cooperatives would include villages, local colleges, panchayats, and SMEs.

They can help in the development of local micro-cell towers and computing servers so that people don't have to stay dependent on distant centres. The government could provide funds and the technical expertise can be attained through partnerships with IITs/ NITs.

This would help to give local ownership, enhance internet access, provide better internet-speed, and prevent monopoly in infrastructure.

6. AI-on-Wheels: Awareness Campaign

No matter how many policies or schemes the government implements, the regulatory hurdles will be there unless the beneficiaries are aware. Mobile vans can be deployed with AI-training kits and regional language instructors, to rotate across 10-15 villages or small towns monthly and organise AI-skilling camps.

As seen in health camps, the AI-skilling camps can make a large section of people in backward areas aware of these skills, technologies, centres, and help in getting more people interested in training. It would help to break infrastructure barriers, even in places where broadband internet is taking time to come up.

Conclusion

AI has the potential to reshape the Indian economy and labour market, but the benefits of this technology will remain constrained to metro cities if not take the right measures at the right time, leading to uneven development and raising the regional disparities. The study shows that while awareness of AI is spreading across all city tiers, meaningful access to training, mentorship, and career opportunities is still concentrated in tier 1 cities. Tier 2 and Tier 3 cities participate more through online courses, yet the lack of local infrastructure, structured guidance, and clear job pathways creates a cycle of dependence on metropolitan centres.

Bridging these divides is now an economic necessity. If India is to realise its full human capital potential and compete globally, they need to invest in region-specific skilling models, improve digital infrastructure, and encourage private players to expand into backward areas. Reducing these regional disparities will ensure that AI becomes a tool for inclusive growth, where talent from smaller towns and rural regions contributes equally to the country's AI-driven transformation.

References

1. Kristalina Georgieva. (2024, January 12). AI will transform the global economy. let's make sure it benefits humanity. International Monetary Fund (IMF).
2. Jiang, S., Pena, Y., Gines, D., Lang, T., Hwang, M., International Economic Development Council, & Economic Development Research Partners. (n.d.). Artificial Intelligence Impact on Labor Markets Literature Review.
3. Purushottam Kaushik, Harsh Sharma, & Ayushi Sarna. (2025, January 22). AI for India 2030: A blueprint for inclusive growth and global leadership. World Economic Forum.
4. Ash. (2025b, May 16). The impact of artificial intelligence on employment in India. IJLSSS.
5. World Economic Forum. (2025). Future of Jobs Report 2025. In I N S I G H T R E P O R T.
6. Data Suggests Growth in Enterprise Adoption of AI is Due to Widespread Deployment by Early Adopters. (2024, January 10). IBM Newsroom.
7. ETtech. (2025, July 29). IT sector hiring rose 5 percent YoY in June; AI, ML see 42 percent spike: Naukri JobSpeak Report. The Economic Times.
8. Mani, V. (2025, July 23). AI talent gap: Savvy freshers bag 4x more pay. The Times of India.
9. D'Monte, L. (2025, April 8). India's AI global profile is rising, but gaps remain, finds Stanford's AI Index report. Mint.
10. India's AI Revolution. (n.d.).
11. Mishra, K., & Srivastava, A. (2024). Impact of artificial intelligence (A.I.) on employment of Indian workers. International Journal for Multidisciplinary Research, 6(5).
12. Cii Team. (2024, November 5). Impact of AI on traditional industries in India: Opportunities and challenges - CII blog. CII Blog.
13. Tewari, T. (2025, September 13). AI hits engineers hard: 67 percent say jobs are changing, 85 percent turn to upskilling. The Times of India.
14. Desk, E., & Manufacturing, E. (2025, July 31). Agentic AI to impact 1.8 crore jobs across manufacturing, retail and education by 2030: Report. ETManufacturing.in.
15. Chakravarty, D. (2025, June 21). Reimagining work in the age of AI: India's opportunity. orfonline.org.

16. Downie, A., & Hayes, M. (2025, April 16). AI in Retail. IBM.
17. Wu Yili. (2023, January 4). Here's how artificial intelligence can benefit the retail sector. World Economic Forum.
18. AI to impact 1.8 crore jobs in manufacturing, retail, education sectors by 2030: Report. (2025, July 29). The Economic Times.
19. AI could reshape half of the roles in India's banking sector: Report. (2025, August 25). The Economic Times.
20. Mr. Sonam Tshewang, Ms. Shreya R Joshi, Mr. Shamanth DR, & Dr. M Govindaraj. (n.d.). Impact of Artificial Intelligence on Job Market in the Banking Sector: A Focus on the Indian Context. In SSRN.
21. Dnyaneshwari Bankar, Swapnil Bawiskar, Yuvraj Bharade, Vidya Bhosale, & Akash Biradar. (n.d.). IMPACT OF AI IN INDIAN EDUCATION SYSTEM. SSRN.
22. Basu, S. (2025, February 27). Rising salaries, evolving work trends: How AI, EV, and engineering sectors are shaping India's job market. The Economic Times.
23. Patra, S. (2025, June 5). How AI is powering India's economic resurgence from tier 2 and 3 cities. Financial Express.
24. Online, I. (2025, July 31). With AI tools, students in Tier 2 and Tier 3 cities can now tell their own stories. The Indian Express.
25. Chaliawala, S. D. N. (2025, August 18). Data centres in non-metro cities a non-starter as AI warrants scale over speed | Mint. Mint.
26. Sharma, S. (2025, July 24). 20 data, AI labs established, 7 more to be added in Tier 2, Tier 3 cities | Latest News India. Hindustan Times.
27. Majumdar, D. (2025, January 24). Emerging jobs in growing Tier 2 and Tier 3 city based tech hubs. The Economic Times.
28. Thomas, S., & Thomas, S. (2025, August 27). One nation, many disconnects: Mapping India's home internet gaps/ » CEDA. CEDA/ ».
29. ET Government & www.ETGovernment.com. (2024, May 14). India needs Rs 4.2L cr investment to connect 24 cr households with broadband by 2030. ETGovernment.com.
30. Parbat, K. (2024, September 14). Rural broadband project lags over planning glitches. The Economic Times.
31. Ghai, N. (2024, January 11). Coursera translates over 4,000 English courses into Hindi using AI. The Economic Times.
32. Online, E. (2025, July 14). Small cities, big growth: Hiring scene hots up in Tier 2, 3 cities. The Economic Times.

CHAPTER 10

Epilogue

Technological advancements have consistently shaped markets, institutions, and social relations. However, artificial intelligence marks a qualitative shift in both scale and speed, fundamentally altering how economic decisions are made, how information is produced and disseminated, and how public and private power is exercised. Unlike earlier waves of digitisation, AI systems increasingly operate autonomously, learn from complex datasets, and generate outcomes that may not be fully anticipated.

As AI becomes embedded across sectors–from pricing algorithms to healthcare diagnostics, content generation, cybersecurity, workforce management and many others–the regulatory challenges it poses are no longer sector-specific or hypothetical. Instead, they are systemic, cross-cutting, and deeply intertwined with questions of market structure, consumer welfare, institutional capacity, and social equity.

India's engagement with AI takes place against a unique backdrop. As a developing economy with a rapidly expanding digital ecosystem, a large and diverse population, and significant developmental aspirations, India must balance the imperatives of innovation, growth, and inclusion with the need to prevent market distortions, violation of rights, and systemic risks. The challenge is not merely to respond to individual harms after they occur, but to design regulatory frameworks that anticipate risk, preserve competition, and ensure that the gains from AI adoption are broadly shared. This requires a holistic whole-of-government approach that brings together competition law, sectoral regulation, data governance, labour policy, and institutional reform.

From a competition law standpoint, AI has begun to reshape the very mechanisms through which coordination and market power emerge. Traditional antitrust enforcement has largely been premised on identifying agreements, intent, and overt conduct among human actors. Algorithm-driven markets complicate this paradigm. Self-learning pricing algorithms, operating in concentrated digital markets, may independently converge on supra-competitive outcomes without explicit communication or collusion in

the conventional sense. As discussed in this report, such tacit algorithmic collusion can emerge rapidly due to repeated interactions, real-time data processing, and feedback loops that reward parallel behaviour.

These challenges established evidentiary standards and raise fundamental questions about how competition law should conceptualise agreement, culpability, and harm in AI-mediated environments.

Indian competition jurisprudence has so far taken a cautious approach. In Samir Agarwal v. ANI Technologies Pvt. Ltd., the Supreme Court declined to characterise algorithmically determined pricing in ride-hailing platforms as a hub-and-spoke cartel, emphasising the absence of inter-driver coordination and the autonomy of individual actors. While this reasoning aligns with existing doctrinal frameworks, it also highlights their limitations when applied to algorithmic systems that influence market outcomes indirectly yet pervasively. As AI-driven pricing and recommendation systems become more sophisticated, reliance solely on traditional concepts of agreement may leave significant anti-competitive conduct beyond the reach of enforcement.

Recognising these emerging challenges, the Competition Commission of India has initiated important capacity-building measures. The establishment of a digital market unit and the release of the Market Study on Artificial Intelligence signal a growing awareness that competition enforcement must evolve alongside technological change. The study's emphasis on self-audits, explainability, transparency, and competition compliance by design reflects a pragmatic attempt to engage with industry while acknowledging enforcement constraints. Similarly, advocacy initiatives and international cooperation efforts demonstrate a willingness to learn from comparative experiences.

However, these steps, while commendable, may not be sufficient on their own. Voluntary compliance mechanisms and ex-post enforcement tools risk being outpaced by the speed and opacity of AI-driven markets. Addressing systemic risks such as tacit algorithmic collusion, data-driven entry barriers, and exclusionary conduct facilitated by AI may require calibrated ex-ante interventions, which may be a soft law in the form of guidelines. These could include enhanced powers for market monitoring, algorithmic auditing under defined safeguards, and the use of regulatory sandboxes or simulation tools to assess potential anti-competitive outcomes before harm materialises. At the same time, any expansion of regulatory powers must be accompanied by strong procedural safeguards, technical expertise, and accountability mechanisms to avoid uncertainty and undue interference with legitimate business innovation.

Beyond competition law, AI presents complex challenges for intellectual property regimes, particularly in the context of generative models trained on vast quantities of copyrighted material. India's copyright framework, while robust in many respects, was not designed for systems that ingest and transform protected works at scale, often without clear attribution or traceability. The resulting tension between fostering AI-driven innovation and protecting the rights and livelihoods of creators has sparked global debate. India's proactive engagement through multi-stakeholder consultations reflects an understanding that rigid or adversarial approaches may be counterproductive.

A balanced path forward requires legal clarity regarding permissible uses of copyrighted material for AI training, including potential exceptions or licensing frameworks for text and data mining. At the same time, the AI industry must assume responsibility for developing technological solutions that mitigate infringement risks, such as improved content filtering, attribution mechanisms, and output controls. Collaboration between policymakers, developers, creators, and legal experts is essential to ensure that India's vibrant creative industries are not marginalised even as its AI ecosystem expands. Such an approach aligns with India's broader objective of promoting innovation while safeguarding cultural and economic diversity.

Sectoral deployment of AI further underscores the need for context-sensitive regulation. In healthcare, for instance, AI-driven tools have the potential to improve diagnostic accuracy, expand access to care, and optimise resource allocation. Yet the risks associated with unregulated deployment are substantial. Algorithms trained on biased or unrepresentative datasets may perpetuate discrimination, while opaque decision-making processes can undermine patient trust and clinical accountability. Errors in AI-assisted diagnosis or treatment recommendations may go undetected, posing serious threats to patient safety. Additionally, the handling of sensitive health data raises acute privacy and security concerns.

These risks are not merely theoretical. In the absence of clear regulatory standards, market incentives may prioritise speed and scale over safety and equity. Moreover, data concentration and proprietary control over AI tools could lead to monopolistic practices that restrict competition and innovation in healthcare delivery. Addressing these challenges requires a robust regulatory framework that incorporates risk-based classification of AI systems, mandatory clinical validation, continuous post-deployment monitoring, and clear rules on liability and informed consent. Coordination between health regulators, data protection authorities, and competition agencies is essential to ensure that AI enhances healthcare outcomes without compromising fundamental rights or market fairness.

Cybersecurity represents another domain where AI's dual-use nature is particularly evident. While AI can strengthen digital defences through automated threat detection and response, it also empowers malicious actors to conduct more sophisticated and scalable attacks. For India, with its rapidly expanding digital infrastructure and diverse threat landscape, the implications are significant. Cyber incidents can disrupt critical services, erode public trust, and impose substantial economic costs. As AI-enabled threats become more prevalent, reactive measures alone will be insufficient.

Building cyber resilience in the age of AI requires sustained investment in research, talent development, and institutional coordination. Regulatory frameworks must encourage transparency, information sharing, and accountability, while avoiding fragmentation and jurisdictional overlap. A whole-of-nation approach—bringing together lawmakers, regulators, industry, and technical experts—is essential to ensure that AI strengthens, rather than undermines, India's digital security architecture.

Perhaps the most far-reaching implications of AI lie in its societal impact. Generative AI systems have demonstrated the capacity to produce misinformation, hallucinations, and biased outputs at scale, with real-world consequences for public discourse, trust, and accountability. In India's socially and linguistically diverse context, these harms are amplified by uneven digital literacy, socio-economic vulnerability, and existing inequalities. Incidents involving AI-generated misinformation have shown how quickly false narratives can spread, undermining confidence in institutions and exacerbating social tensions.

India's current legal framework offers only partial responses to these challenges. While statutes such as the IT Act and the Digital Personal Data Protection Act provide some safeguards, they were not designed for autonomous, probabilistic systems that blur traditional notions of authorship and responsibility. Regulatory responses have largely been reactive, relying on advisories, platform compliance, and post-hoc enforcement. Binding obligations for algorithmic accountability, pre-deployment risk assessment, and clear liability allocation remain underdeveloped. In such an environment, harms are often addressed only after they have already caused widespread damage.

At the same time, regulation cannot rely solely on restriction. India's ambition to leverage AI for development, productivity, and public service delivery is both legitimate and necessary. AI holds promise for improving governance, expanding access to education and healthcare, and addressing long-standing developmental challenges. The task, therefore, is to align this ambition with safeguards that reflect India's socio-economic realities. This requires a layered governance approach that combines technical standards, legal obligations,

competition remedies, and public investment in capacity-building. Without parallel efforts to expand access to compute infrastructure, local datasets, auditing capabilities, and digital literacy, even well-intentioned regulation risks reinforcing incumbent advantages and excluding smaller innovators.

The distributive effects of AI adoption are particularly evident in the labour market. While AI has the potential to generate new forms of employment and enhance productivity, its benefits risk being geographically and socially concentrated. Evidence indicates that meaningful access to AI training, mentorship, and career opportunities remains largely confined to metropolitan centres. Tier 2 and Tier 3 cities, as well as rural regions, often lack the infrastructure and institutional support needed to translate online learning into sustainable employment. This concentration threatens to exacerbate regional disparities and undermine India's broader development goals.

Addressing these challenges requires targeted policy interventions. Region-specific skilling initiatives, improved digital infrastructure, and incentives for industry participation beyond major urban centres are essential. Collaboration between government, educational institutions, and private sector actors can help build local ecosystems that support AI-driven employment and entrepreneurship. Ensuring that AI becomes a tool for inclusive growth rather than a driver of inequality is not merely a social imperative but a strategic economic necessity.

Artificial Intelligence: Minimising Risks and Maximising Gains

Taken together, the themes explored in this report point to a central conclusion: the risks and rewards of AI are inseparable from questions of institutional design and governance capacity. Fragmented regulatory approaches, whether through isolated sectoral interventions or reliance on *ex-post* remedies, are ill-suited to the systemic nature of AI-related challenges. Effective governance requires coherence across competition law, sectoral regulation, data protection, labour policy, and cybersecurity. Institutionalised mechanisms for inter-regulatory coordination, stakeholder consultation, and regulatory impact assessment are critical to achieving this coherence.

Strengthening state capacity is equally important. Regulators must be equipped with the technical expertise, data access, and analytical tools necessary to understand and respond to AI-driven markets. Investment in research, training, and international cooperation can help bridge existing capability gaps. At the same time, accountability mechanisms through parliamentary oversight, judicial review, and transparent decision-making must ensure that expanded regulatory powers are exercised responsibly.

Industry also has a vital role to play. Responsible innovation, compliance-by-design, and constructive engagement with regulators are essential to building trust and legitimacy. Firms that deploy AI systems must recognise that automation does not absolve responsibility; rather, it heightens the need for oversight and ethical consideration. Clear regulatory expectations, combined with collaborative governance mechanisms, can help align private incentives with public objectives.

As India stands at this critical juncture, the choice is not between innovation and regulation, but between fragmented, reactive governance and a coherent, forward-looking framework that integrates the two. Treating AI as essential economic and social infrastructure demands oversight, accountability, and inclusive access. By strengthening competition frameworks, aligning sectoral regulations, and investing in institutional capacity, India can harness AI as a catalyst for growth, welfare, and resilience. The decisions taken today will shape not only the trajectory of India's AI ecosystem but also the character of its digital economy and social contract in the time to come.

Looking ahead, a central question that will shape policy choices over the coming years is whether the current trajectory of AI represents a temporary wave of technological exuberance or a deeper, structural transformation of the economy and society. The answer is unlikely to be binary. Rather than framing AI as either hype or inevitability, policymakers should treat it as a set of general-purpose technologies whose long-term significance will be revealed through sustained, observable outcomes.

Durable productivity gains across sectors, persistent changes in market structure and business models, broad-based labour reallocation accompanied by meaningful job creation, and the stable integration of AI into public service delivery would point to structural change. Conversely, repeated cycles of inflated expectations followed by retrenchment—where investment growth, valuations, and deployment announcements consistently outpace real-world impact—would signal a corrective phase.

In this context, the capacity to monitor, measure, and adapt becomes as important as the content of regulation itself. A limited set of public indicators — such as concentration in compute and model access, the ratio of large-scale deployments to independent impact assessments, the openness or closure of foundational models, the frequency and severity of adverse incidents in high-risk sectors, and the geographic distribution of AI-related investment and employment—can provide early signals of both promise and risk. Treating such monitoring as a form of public infrastructure would allow regulators to calibrate interventions, distinguish structural shifts from speculative excess, and avoid both premature over-regulation and delayed response.

Looking further ahead, policymakers would benefit from stress-testing AI governance against a small number of plausible scenarios rather than assuming a single trajectory. One pathway involves inclusive integration, where public investment in capacity, targeted guardrails, and institutional coordination enable widespread adoption and decentralised gains. Another points toward winner-takes-most outcomes, driven by concentration of compute, data, and proprietary models, with implications for competition and innovation. A third, less desirable scenario involves regulatory shock, triggered by a major safety failure or misuse event that erodes public trust and prompts abrupt, restrictive intervention. Preparing for these possibilities requires flexibility, sequencing, and institutional resilience rather than rigid rule-making alone.

Ultimately, the future of AI in India will be shaped less by technological capability alone than by choices about governance, measurement, and inclusion. By investing in monitoring capacity, prioritising a small number of durable guardrails, and strengthening coordination across institutions, India can navigate uncertainty without forfeiting opportunity. Whether AI proves to be a passing surge or a foundational transformation, a governance framework that is adaptive, evidence-based, and attentive to distributional consequences will remain valuable long after specific technologies evolve.