Equi Corp Associates
Advocates & Solicitors
TRANSACTION • ADVISORY • LITIGATION

EquiCorp
ASSOCIATES LLP

REGULATORY FRAMEWORK FOR
ARTIFICIAL INTELLIGENCE
BUSINESSES IN INDIA

A Comprehensive Legal & Regulatory Compendium

2026

Covering Regulations of:

MeitY • SEBI • RBI • CCI • TRAI • IRDAI • PRDAI • PFRDA • IT Act

EQUICORP ASSOCIATES LLP

Advocates & Solicitors

www.equicorplegal.com

FOREWORD

The emergence of artificial intelligence as a transformative technological force has confronted legal systems around the world with challenges of an unprecedented character. In India, the intersection of a dynamic digital economy, a sophisticated constitutional framework, and a complex multi-regulator architecture have made the governance of AI a subject of acute professional importance. Yet, until now, practitioners navigating this space have lacked a single, authoritative compendium that draws together the full landscape of applicable law and regulation.

This volume fills that gap. Conceived and produced by the lawyers at EquiCorp Associates LLP, the Regulatory Framework for Artificial Intelligence Businesses in India offers the practitioner, in-house counsel, policy specialist, and scholar alike a systematic account of the law as it stands, organised around the regulatory pillars that govern AI deployment across India's principal sectors.

The approach adopted is deliberately pluralist. Artificial intelligence does not respect the jurisdictional siloes that structure Indian regulatory law; a single deployed AI system may simultaneously engage the data protection obligations administered by the Data Protection Board, the financial sector conduct standards of the Securities and Exchange Board of India and the Reserve Bank of India, the competition law framework enforced by the Competition Commission of India, the telecommunications infrastructure oversight of TRAI, and the overarching information technology framework of MeitY. This compendium maps all of these intersections with care.

Equally important is the treatment of judicial precedent. The Supreme Court of India and its High Courts have, across a range of fields, developed doctrinal positions of direct relevance to AI governance even in the absence of AI-specific legislation. Privacy, automated decision-making, algorithmic accountability, platform liability, and consumer protection have all received authoritative treatment in Indian courts. This volume extracts and analyses the ratio decidendi of those decisions, enabling practitioners to deploy established doctrine in novel contexts.

The authors have proceeded on the premise that the law applicable to AI businesses in India is not yet settled, and that intellectual honesty demands candid acknowledgment of lacunae and

areas of regulatory uncertainty. Where the law is clear, it is stated plainly. Where it is contested, competing positions are identified and evaluated. Where it is absent, the volume identifies the gap and, where appropriate, draws on comparative and international frameworks to suggest how Indian law might develop.

It is hoped that this work will serve as a reliable starting point for the many lawyers, regulators, entrepreneurs, and policymakers who must navigate this complex and rapidly evolving field.

EquiCorp Associates LLP

New Delhi, 2026

TABLE OF ABBREVIATIONS

ADM Jabalpur	Additional District Magistrate, Jabalpur v. Shivkant Shukla
AIF	Alternative Investment Fund
AI	Artificial Intelligence
AIML	Artificial Intelligence and Machine Learning
AIR	All India Reporter
AMI	Advanced Metering Infrastructure
AMLA	Anti-Money Laundering Act
API	Application Programming Interface
BFSI	Banking, Financial Services & Insurance
BNSS	Bharatiya Nagarik Suraksha Sanhita, 2023
BRO	Body-Worn Camera Recording Obligation
CCI	Competition Commission of India
CPC	Code of Civil Procedure, 1908
CERT-In	Computer Emergency Response Team – India
CKYC	Central Know Your Customer Registry
CRA	Credit Rating Agency
DPDPA	Digital Personal Data Protection Act, 2023
DPDPB	Data Protection Board of India
DSP	Digital Services Provider
ESOP	Employee Stock Ownership Plan
FATF	Financial Action Task Force
FDI	Foreign Direct Investment

FEMA	Foreign Exchange Management Act, 1999
FinTech	Financial Technology
GDPR	General Data Protection Regulation (EU)
GenAI	Generative Artificial Intelligence
IBBI	Insolvency and Bankruptcy Board of India
IBC	Insolvency and Bankruptcy Code, 2016
IEA	Indian Evidence Act, 1872 / Bharatiya Sakshya Adhiniyam, 2023
IPC	Indian Penal Code, 1860 / Bharatiya Nyaya Sanhita, 2023
IRDAI	Insurance Regulatory and Development Authority of India
IT Act	Information Technology Act, 2000
ITAA	Information Technology (Amendment) Act, 2008
KYC	Know Your Customer
LLM	Large Language Model
MCA	Ministry of Corporate Affairs
MeitY	Ministry of Electronics and Information Technology
ML	Machine Learning
NLP	Natural Language Processing
NPCI	National Payments Corporation of India
OTP	One-Time Password
PFRDA	Pension Fund Regulatory and Development Authority
PIB	Press Information Bureau
PMLA	Prevention of Money Laundering Act, 2002
PPI	Prepaid Payment Instrument
RBI	Reserve Bank of India

SEBI	Securities and Exchange Board of India
SPDI	Sensitive Personal Data or Information
SRO	Self-Regulatory Organisation
TOC	Terms of Contract
TRAI	Telecom Regulatory Authority of India
UCC	Unsolicited Commercial Communication
UPI	Unified Payments Interface
WPC	Wireless Planning and Coordination Wing

TABLE OF CONTENTS

CHAPTER ONE

The Regulatory Landscape for Artificial Intelligence in India: An Introduction

1.1 The Emergence of Artificial Intelligence as a Regulatory Subject

Artificial intelligence has, within the span of a single decade, transitioned from the domain of specialist academic inquiry to a pervasive component of commercial, financial, and governmental activity. In India, this transformation has been particularly rapid. The country has embraced AI as a strategic national priority, reflected in a succession of policy instruments commencing with the National Strategy for Artificial Intelligence issued by Niti Aayog in 2018.[1]

The NASSCOM AI Adoption Index of 2024 estimated that India had become the third-largest AI talent pool globally, with AI technology adoption accelerating across the banking, financial services and insurance (BFSI) sector, healthcare, agriculture, logistics, and public administration.[2]

Yet the enthusiasm for AI deployment has proceeded without a comprehensive, sector-neutral legislative framework. Unlike the European Union, which enacted its AI Act in June 2024, India has proceeded through a combination of sectoral regulation, advisory instruments, and interpretive expansion of existing statutes.[3]

The regulatory practitioner must therefore navigate a landscape that is simultaneously densely populated with applicable rules and perforated by significant gaps. This compendium is designed to serve as an authoritative map of that landscape.

1.1.1 National AI Policy Architecture

[1]Niti Aayog, "National Strategy for Artificial Intelligence #AIforAll" (Government of India, 2018) 7–12.

[2]NASSCOM, "AI Adoption Index India 2024" (NASSCOM, 2024) 3.

[3]European Parliament and Council, Regulation (EU) 2024/1689 of 13 June 2024 laying down harmonised rules on artificial intelligence (AI Act) [2024] OJ L1689 (the "EU AI Act").

The principal policy documents governing AI in India are the Niti Aayog's 2018 National Strategy for AI, the 2021 document on Responsible AI for All, and the MeitY Expert Committee Interim Report of February 2024.[4]

The responsible AI principles articulated by Niti Aayog — safety and reliability, equality, inclusivity and non-discrimination, privacy and security, transparency, accountability, and protection and reinforcement of positive human values — constitute soft law of significant interpretive relevance.[5]

These documents, while not having the force of subordinate legislation, are routinely cited in regulatory consultations, compliance frameworks, and increasingly in court submissions as evidence of the State's declared policy on AI governance. A practitioner who ignores them does so at the risk of failing to understand the direction of regulatory travel.

1.2 Constitutional Foundations for AI Regulation

The constitutional basis for AI regulation in India derives from multiple provisions of the Constitution of India, 1950. The most directly relevant are Articles 14, 19, and 21, whose interaction with digital technology and automated decision-making has been progressively illuminated by the Supreme Court.[6]

1.2.1 Article 21 and the Right to Privacy

The foundational case is Justice K.S. Puttaswamy (Retd.) v. Union of India, where a nine-judge bench of the Supreme Court unanimously held that the right to privacy is a fundamental right under Article 21 of the Constitution.[7]

Justice K.S. Puttaswamy (Retd.) v. Union of India	
Citation	(2017) 10 SCC 1
Forum	Supreme Court of India (Nine-Judge Bench)

[4]Expert Committee on AI Governance, Interim Report (MeitY, February 2024).

[5]Niti Aayog, "Responsible AI for All: Implementing the Principles – A Use Case Approach" (Government of India, 2021) 11.

[6]Justice K.S. Puttaswamy (Retd.) v. Union of India, (2017) 10 SCC 1 (India).

Year	2017

Ratio Decidendi

The right to privacy is an intrinsic part of the right to life and personal liberty guaranteed under Article 21 of the Constitution of India. Privacy includes within its compass the right to informational self-determination, protection of personal identity, decisional autonomy, and the right to be left alone. The State must satisfy the three-pronged test of legality, necessity, and proportionality to justify any infringement of the privacy right.

Regulatory Significance: Foundational authority for all AI regulation involving personal data processing, automated profiling, and algorithmic decision-making. The proportionality standard derived from Puttaswamy is the constitutional benchmark against which regulatory obligations imposed on AI businesses are measured.

The Puttaswamy judgment is the constitutional cornerstone of AI regulation in India. Its nine separate opinions, read together, establish that informational privacy — the right to control data about oneself — is constitutionally protected. Any statutory scheme that permits automated processing of personal data, algorithmic profiling, or AI-generated decisions affecting individuals must satisfy the proportionality test.[8]

The subsequent decision in Maneka Gandhi establishes that Article 21 requires not merely procedural fairness but substantive due process. Applied to AI contexts, this principle has been invoked to argue that algorithmic decisions affecting a person's liberty, livelihood, or dignity must be preceded by a fair procedure and must not be arbitrary.[9]

1.2.2 Article 14 and Algorithmic Arbitrariness

Article 14 of the Constitution guarantees the right to equality and prohibits arbitrary State action. The Supreme Court in Shayara Bano developed the doctrine of manifest arbitrariness, holding that legislation or state action that is excessive, capricious, or irrational without adequate determining principle is liable to be struck down.[10]

[9]Maneka Gandhi v. Union of India, (1978) 1 SCC 248 (India) (establishing that Art. 21 embodies a guarantee of substantive and procedural fairness).

[10]Shayara Bano v. Union of India, (2017) 9 SCC 1 (India) (on manifest arbitrariness as a ground for invalidating legislation under Art. 14).

Shayara Bano v. Union of India	
Citation	(2017) 9 SCC 1
Forum	Supreme Court of India (Five-Judge Bench)
Year	2017

Ratio Decidendi

Manifest arbitrariness, established as a ground for striking down legislation under Article 14, requires that the law or action be capricious, irrational, or disproportionate without any adequate determining principle. The doctrine applies to both legislative and executive action and provides a ground of challenge independent of reasonable classification under Article 14.

Regulatory Significance: The manifest arbitrariness doctrine is directly applicable to challenges against AI systems that produce outcomes affecting citizens without transparent decision criteria. Where a public authority deploys an AI system whose outputs are opaque or whose design lacks a rational determining principle, Article 14 challenges become available.

The intersection of Article 14 with algorithmic decision-making is of acute practical importance. Where a government agency uses an AI system to determine benefits entitlement, tax compliance risk scores, or immigration decisions, the absence of explainability and the opacity of the algorithm may constitute manifest arbitrariness. The doctrine requires that the AI system's decision criteria be grounded in a rational and publicly articulable principle.[11]

1.2.3 Article 19 and Freedom of Expression

Article 19(1)(a) guarantees freedom of speech and expression. The deployment of AI in content moderation, automated censorship, deepfake detection and removal, and recommendation systems directly engages this right. The Supreme Court in Anuradha Bhasin held that restrictions on digital communication must satisfy the proportionality standard: any such restriction must be (i) prescribed by law; (ii) necessary to achieve a legitimate aim; and (iii) proportionate to the threat addressed.[12]

[12]Anuradha Bhasin v. Union of India, (2020) 3 SCC 637 (India) (establishing proportionality as a standard for internet-related restrictions under Art. 19).

Anuradha Bhasin v. Union of India	
Citation	(2020) 3 SCC 637
Forum	Supreme Court of India
Year	2020

Ratio Decidendi

Any restriction on internet access or digital communication must be (i) sanctioned by law; (ii) in pursuit of a legitimate aim; and (iii) proportionate, i.e., not exceeding what is necessary to achieve the aim. Orders imposing such restrictions must be published and subject to judicial review.

Regulatory Significance: Directly applicable to the design of AI-powered content moderation systems and automated takedown tools. A content moderation AI must be capable of principled, proportionate, and reviewable decision-making to satisfy constitutional standards.

1.3 Definitional Framework: What Is "Artificial Intelligence" in Indian Law?

Indian law does not yet contain a single, authoritative legislative definition of artificial intelligence. This creates interpretive complexity, since the application of existing statutes and regulations to AI systems depends upon whether those systems fall within their operative definitions.[13]

The ISO/IEC 22989:2022 standard defines an "AI system" as "an engineered system that generates outputs such as content, forecasts, recommendations, or decisions for a given set of human-defined objectives." This functional definition — emphasising outputs rather than architecture — has been influential in Indian regulatory instruments.[14]

The Niti Aayog's Responsible AI principles adopt a broadly consistent approach, defining AI as technology that enables machines to perform tasks that would otherwise require human

[13]ISO/IEC 22989:2022, "Artificial Intelligence — Concepts and Terminology" (International Organization for Standardization, 2022).

intelligence, including learning, reasoning, problem-solving, perception, and language understanding.[15]

1.3.1 Sectoral Definitions

Several Indian regulators have issued working definitions for AI within their respective domains. The RBI's Draft IT Governance Directions define "Artificial Intelligence and Machine Learning" as "a set of technologies that enable computers to perform tasks that typically require human intelligence."[16]

SEBI's 2019 AI/ML Circular does not define AI or ML directly, but treats them as sub-categories of algorithms, and accordingly subjects them to the framework applicable to algorithmic trading.[17]

The DPDPA 2023 does not define AI or automated decision-making as a standalone concept, though Section 2(h) and related provisions create obligations that apply wherever personal data is processed algorithmically.[18]

1.3.2 Interpretive Approach in the Absence of a Statutory Definition

In the absence of a comprehensive statutory definition, courts and regulators have approached AI systems through the lens of existing definitional categories. The IT Act 2000 defines "computer" in Section 2(i) as including "any electronic, magnetic, optical or other high-speed data processing device or system which performs logical, arithmetic, and memory functions by manipulations of electronic, magnetic or optical impulses." An AI system, operating on digital hardware, falls squarely within this definition.[19]

[15]Niti Aayog, "Principles for Responsible AI" (Government of India, 2021) 9 (defining "Artificial Intelligence System" functionally, by reference to the capacity to generate outputs that influence environments).

[16]Reserve Bank of India, "Draft Master Direction – Information Technology Governance, Risk, Controls and Assurance Practices" (November 2023) para 8 (defining "Artificial Intelligence and Machine Learning" in a banking context).

[17]SEBI, "Circular on Usage of Artificial Intelligence and Machine Learning Applications by SEBI Registered Intermediaries" (Circular No. SEBI/HO/MIRSD/TPD/CIR/P/2019/135, 4 November 2019).

[18]Digital Personal Data Protection Act, 2023, No. 22 of 2023 (India), s 2(h) (defining "data principal") and s 2(i) (defining "data fiduciary").

[19]Information Technology Act, 2000, No. 21 of 2000 (India), as amended by the Information Technology (Amendment) Act, 2008.

The principle of eiusdem generis and the canon of technology-neutral statutory interpretation support an expansive reading of "computer" and related definitions to encompass AI systems, including large language models and neural networks.[20]

1.4 The Multi-Regulator Architecture

The regulatory architecture governing AI businesses in India is characterised by a plurality of competent authorities, each exercising jurisdiction over AI systems deployed within their respective domains. Understanding this architecture is indispensable to compliance planning.[21]

1.4.1 MeitY

The Ministry of Electronics and Information Technology (MeitY) is the apex policy authority for the information technology sector. MeitY exercises regulatory functions under the IT Act 2000 and is the authority responsible for administering the DPDPA 2023. Its advisory of March 2024 on AI platforms is the most direct governmental expression of AI-specific regulatory expectations.[22]

1.4.2 SEBI

The Securities and Exchange Board of India (SEBI) exercises jurisdiction over AI systems deployed in securities markets, including algorithmic trading, robo-advisory services, AI-powered research analytics, and fraud surveillance. SEBI's regulatory framework for algorithmic trading has served as the de facto regime for AI in capital markets.

1.4.3 RBI

The Reserve Bank of India (RBI) regulates AI deployment in the banking, payment, and lending sectors. Its regulatory toolkit includes Directions under the RBI Act 1934, the Banking Regulation Act 1949, and the Payment and Settlement Systems Act 2007. The RBI's focus has been on AI used in credit decisioning, fraud detection, and payment systems.

1.4.4 CCI

[20]Cf. Shivaji Rao Patil v. Mahesh Madhav Gosavi, (1987) 2 SCC 484 (India) (strict statutory interpretation; eiusdem generis canon); applied by analogy to technology-neutral statutory definitions.

[22]MeitY, "Advisory for Intermediaries and Platforms on Use of AI" (1 March 2024) (subsequently clarified on 15 March 2024).

The Competition Commission of India (CCI) reviews the competition law dimensions of AI: the use of algorithmic pricing, AI-enabled data concentration, and the competitive implications of platform AI systems. The CCI's Market Study on the Telecom Sector and its evolving jurisprudence on platform markets are of direct relevance.

1.4.5 TRAI

The Telecom Regulatory Authority of India (TRAI) regulates AI systems deployed in telecommunications infrastructure, including AI-driven network management, automated spam filtering, and algorithmic customer service tools deployed by telecom operators.

1.4.6 IRDAI and PFRDA

The Insurance Regulatory and Development Authority of India (IRDAI) and the Pension Fund Regulatory and Development Authority (PFRDA) exercise oversight over AI systems in the insurance and pension sectors respectively, with particular attention to AI-powered underwriting, claims assessment, and investment management.

1.5 Structure of This Compendium

This compendium is organised in fourteen chapters, each addressing a distinct pillar of the regulatory framework for AI businesses in India. The chapters proceed from the constitutional and policy foundations, through the principal sectoral regimes, to specialist topics including competition law, criminal liability, and international dimensions.

Chapter Two addresses the Digital Personal Data Protection Act 2023, which constitutes the primary data law applicable to AI systems processing personal data. Chapter Three covers the IT Act framework, including intermediary liability and cybersecurity obligations. Chapters Four through Seven address the financial sector regulators — SEBI, RBI, IRDAI, and PFRDA. Chapter Eight analyses the CCI's competition law framework. Chapter Nine covers TRAI's regulatory framework. Chapters Ten and Eleven address sector-specific topics in healthcare AI and public sector AI respectively. Chapter Twelve covers criminal liability and forensic AI. Chapter Thirteen addresses contractual and intellectual property dimensions. Chapter Fourteen surveys international frameworks and India's engagement with global AI governance.

Each chapter follows a consistent structure: an introduction to the regulatory domain, a systematic analysis of applicable rules and standards, a case law analysis featuring the ratio decidendi of relevant decisions, a consolidated regulatory matrix, and a practitioner's checklist.

1.6 Compliance Matrix: Constitutional and Policy Foundations

The following compliance matrix sets out the key obligations, applicable legal instruments, required standards, risk classifications, and mandatory actions for entities operating in this regulatory domain:

Compliance Obligation	Legal Instrument	Standard / Threshold	Risk Level	Required Action
Privacy Impact Assessment for AI systems processing personal data	Art. 21, Constitution; Puttaswamy (2017) 10 SCC 1	Proportionality — legality, necessity, proportionate means	**Critical**	Conduct PIA before deployment of any AI system processing personal data; document constitutional justification
Fairness and non-arbitrariness in AI decision outputs	Art. 14, Constitution; Shayara Bano (2017) 9 SCC 1	Manifest arbitrariness — rational determining principle required	**High**	Document the decision criteria and rational basis for all AI systems making decisions affecting individuals; implement explainability mechanisms
Proportionality of AI content	Art. 19(1)(a); Anuradha	Restriction must be (i) in law; (ii) legitimate aim;	**High**	Ensure AI content moderation is legally authorised, pursues a

Compliance Obligation	Legal Instrument	Standard / Threshold	Risk Level	Required Action
moderation systems	Bhasin (2020) 3 SCC 637	(iii) proportionate		legitimate aim, and is not overbroad; implement appeal/review mechanism
Compliance with Responsible AI Principles (soft law)	Niti Aayog, Responsible AI for All (2021)	Safety, fairness, accountability, transparency, privacy	**Medium**	Map AI governance framework to Niti Aayog principles; document compliance in board-level AI policy
Engagement with MeitY AI advisories	MeitY Advisory (March 2024); IT Act s 87	Compliance with MeitY directions as issued	**High**	Monitor MeitY advisory publications; assess applicability to deployed AI systems; maintain compliance register
AI definitional classification for regulatory purposes	IT Act s 2(i); ISO/IEC 22989:2022; sectoral definitions	Functional definition — systems generating outputs requiring human intelligence	**Medium**	Classify each AI system under applicable sectoral definitions; identify primary regulator; document classification rationale

Compliance Obligation	Legal Instrument	Standard / Threshold	Risk Level	Required Action
Multi-regulator jurisdiction mapping	SEBI Act; RBI Act; Competition Act; TRAI Act; DPDPA; IT Act	Identify all regulators with jurisdiction over each AI deployment	High	Prepare a jurisdiction map for each AI product/service; assign compliance owner per regulator; review annually

CHAPTER TWO

The Digital Personal Data Protection Act, 2023: Implications for Artificial Intelligence

2.1 Introduction and Legislative Context

The Digital Personal Data Protection Act, 2023 (DPDPA) received presidential assent on 11 August 2023 and represents India's first comprehensive data protection legislation. For AI businesses, the DPDPA is the primary statutory instrument governing the collection, use, and processing of personal data in the training, deployment, and operation of AI systems.[23]

The Act proceeds from the constitutional foundation laid in Puttaswamy and establishes a data fiduciary–data principal framework that has direct and substantial implications for AI developers, platform operators, and data aggregators. Understanding the DPDPA's architecture is indispensable for any AI business operating in India.

The DPDPA follows a principles-based model: it enacts a small number of high-level obligations and confers broad delegated rulemaking powers on the Central Government. As of the date of this publication, the implementing rules have not been finalised; practitioners must therefore read the Act together with the draft rules and any advisories issued by MeitY.

MeitY / DPDPB — Digital Personal Data Protection Act, 2023 (2023)

Establishes a data fiduciary–data principal framework applicable to the processing of digital personal data within India, and to processing outside India where the data principal is in India. Imposes obligations of notice, consent, purpose limitation, data minimisation, storage limitation, accuracy, security, and accountability. Creates the Data Protection Board as the adjudicatory authority. Provides for cross-border data transfer subject to government notification.

2.2 Applicability to AI Systems

2.2.1 "Processing" of Personal Data by AI Systems

[23] Digital Personal Data Protection Act, 2023, No. 22 of 2023 (India) (hereinafter "DPDPA 2023").

The DPDPA applies to "processing" of "personal data," defined broadly to include collection, storage, use, sharing, and deletion. Any AI system that ingests personal data — whether in training datasets, fine-tuning processes, inference pipelines, or output generation — is engaged in "processing" within the meaning of the Act.[24]

The critical question for AI practitioners is whether training data — often scraped from public internet sources — constitutes personal data and whether its use for model training requires a lawful basis. The Act defines "personal data" as "any data about an individual who is identifiable by or in relation to such data." The inclusion of indirectly identifiable data within this definition means that training datasets that include names, identifiers, online behaviour, or other individually attributable information will typically constitute personal data.

2.2.2 Data Fiduciary Classification for AI Businesses

Under the DPDPA, an AI business that determines the "purpose and means of processing" personal data is a "data fiduciary" and bears the primary obligations under the Act. An AI company that processes personal data on behalf of another entity as directed by that entity is a "data processor" and has more limited statutory obligations.[25]

The classification of an AI company as fiduciary or processor has major compliance implications. A foundation model developer that trains models on user data and determines what data to collect and how to use it is a data fiduciary. A company that provides an AI inference API where the customer controls data input and use is more likely a data processor, though the facts must be examined in each case.

2.2.3 Significant Data Fiduciary Status

Section 10 of the DPDPA provides for the designation of certain data fiduciaries as "Significant Data Fiduciaries" (SDFs) on the basis of volume and sensitivity of personal data processed, risk to rights of data principals, national security implications, public order, or risk to electoral democracy. SDFs face heightened obligations including mandatory data protection impact assessments, appointment of a Data Protection Officer, and periodic audit requirements.[26]

[24]DPDPA 2023, s 4 (grounds for processing personal data).

[25]DPDPA 2023, ss 8–9 (obligations of data fiduciary).

[26]DPDPA 2023, s 10 (significant data fiduciary).

Large AI platforms, foundational model developers, and AI-driven social media and search systems are candidates for SDF designation. Practitioners advising such clients must monitor the SDF designation notifications closely, as they carry substantial compliance obligations.

2.3 Lawful Grounds for AI Data Processing

2.3.1 Consent

Section 6 of the DPDPA requires that consent for data processing be free, specific, informed, unconditional, and unambiguous, signified through a clear affirmative action. For AI businesses, this standard raises significant challenges. Training data scraped from public internet sources was not obtained with consent meeting the DPDPA standard. Fine-tuned models trained on user interactions require that users have consented specifically to use of their data for training purposes.[27]

2.3.2 Legitimate Use without Consent

Section 7 provides for "deemed consent" in specified circumstances, including processing "for the performance of any function under any law," "for the purposes of employment," and "for medical emergency." Additionally, Section 7(j) provides for processing for legitimate interests — a provision of potentially broad application to AI systems providing personalised services.[28]

2.3.3 AI Training Data: The Consent Problem

The central unsolved problem in Indian AI data law is whether the processing of publicly available data for AI model training requires individual consent. The DPDPA does not include an explicit provision analogous to the GDPR's research exception or the UK GDPR's "legitimate interests" balancing test as applied to publicly available data.

Practitioners advising AI developers must consider: (a) whether training data has been sourced lawfully; (b) whether the data includes personal data as defined in the Act; (c) if so, whether a lawful ground under Section 7 is available; and (d) whether the data principal's right to erasure (Section 12(d)) could be asserted against a trained model, requiring data deletion procedures.

[27]DPDPA 2023, s 6 (consent).

[28]DPDPA 2023, s 11 (deemed consent).

2.4 Rights of Data Principals and AI Decision-Making

2.4.1 Rights Architecture

Chapter III of the DPDPA confers upon data principals the rights of (i) information about processing; (ii) correction and erasure; (iii) grievance redressal; and (iv) nomination. These rights apply wherever an AI system processes personal data.[29]

2.4.2 No Explicit Right to Explanation or Human Review

The DPDPA does not, unlike the EU GDPR Article 22, confer an explicit right not to be subject to automated decision-making or a right to human review of automated decisions. This is a significant lacuna. The absence of an explicit automated decision-making provision means that challenges to AI-generated decisions affecting data principals must proceed under the general rights framework of the Act or through constitutional channels.[30]

However, the combination of the right to information (which includes information about the logic of data processing) and the grievance redressal right (which requires the data fiduciary to address complaints about processing) creates an implied obligation on AI businesses to be capable of explaining their decisions and addressing complaints about automated outputs.

2.4.3 The Erasure Right and AI Models

Section 12(b) provides for the right to erasure of personal data where the data principal withdraws consent or the processing purpose is no longer served. Applied to AI systems, this right creates the "right to be forgotten from the model" problem: where a data principal's data was used in model training, can they require erasure of their data from the trained model? Technically, individual data records cannot be "erased" from a trained neural network without model retraining. The Act does not address this question, which will require regulatory clarification.[31]

Karmanya Singh Sareen v. Union of India	
Citation	(2017) 239 DLT 537
Forum	Delhi High Court (Division Bench)
Year	2017

[29]DPDPA 2023, s 12 (rights of data principal).

[30]Cf. GDPR, Art. 22 (automated individual decision-making); see also Information Commissioner's Office (UK), "Guidance on Automated Decision-Making" (ICO, 2023) for comparative analysis.

Ratio Decidendi

The sharing of personal data collected under one privacy policy with a third party under materially different terms, without renewed, specific, and informed consent, violates the right to informational privacy protected under Article 21. A data controller cannot unilaterally alter the basis on which data was originally collected. The court recognised that privacy in digital communications is both an individual and collective right of significance.

Regulatory Significance: Applicable to AI platforms that process user data under terms of service that do not specifically disclose AI training use. Companies migrating user data from pre-DPDPA collection to AI training pipelines without fresh consent face significant liability exposure.

2.5 Data Localisation and Cross-Border AI Processing

Section 16 of the DPDPA authorises the Central Government to restrict transfers of personal data to specified countries by notification. The Act adopts an allowlist model: transfers are permitted to countries not on the restricted list. This framework has major implications for AI companies that process Indian user data on servers outside India, use cross-border cloud AI inference, or share training data with overseas affiliates.[32]

The government has not, at the time of writing, issued the allowlist notification. Until it does, the cross-border transfer restriction is not operative. Practitioners should monitor MeitY notifications closely. The allowlist approach, if implemented restrictively, could significantly constrain AI businesses that rely on cross-border data flows for model development and inference.

2.6 Children's Data and AI Systems

Section 9 of the DPDPA contains heightened obligations in respect of personal data of children (persons under 18 years). Data fiduciaries must obtain verifiable parental consent before processing a child's personal data and must not undertake any processing that is detrimental to the child's well-being or engage in behavioural monitoring or targeted advertising directed at children.[33]

These provisions have direct implications for AI systems deployed in EdTech, gaming, and social media contexts that may serve minors. The prohibition on behavioural monitoring and targeted

[32]DPDPA 2023, s 16 (transfer of personal data outside India).

[33]DPDPA 2023, s 9 (processing of children's personal data).

advertising using children's data effectively prohibits personalised recommendation AI for users under 18 in the absence of parental consent.

2.7 Penalties and Enforcement

Schedule I of the DPDPA prescribes civil penalties of up to INR 250 crore for certain categories of breach, including failure to take reasonable security safeguards and failure to notify the Data Protection Board of a personal data breach. The Data Protection Board, established under Section 33, is the adjudicatory authority.[34]

For AI businesses, the most financially significant penalty risk arises from: (a) processing personal data in training datasets without lawful basis; (b) failure to implement security safeguards proportionate to the sensitivity of data processed; (c) failure to honour data principal rights; and (d) unlawful cross-border data transfers.

2.8 Compliance Matrix: DPDPA 2023 and AI Data Processing

The following compliance matrix sets out the key obligations, applicable legal instruments, required standards, risk classifications, and mandatory actions for entities operating in this regulatory domain:

Compliance Obligation	Legal Instrument	Standard / Threshold	Risk Level	Required Action
Lawful basis for AI training data processing	DPDPA 2023, ss 6-7	Consent (s 6) or deemed consent / legitimate use (s 7); specific, informed, unconditional	**Critical**	Audit training datasets; obtain DPDPA-compliant consent or identify s 7 ground; document and maintain consent records

[34] DPDPA 2023, s 25 (offences and penalties — financial penalties up to INR 250 crore).

Compliance Obligation	Legal Instrument	Standard / Threshold	Risk Level	Required Action
Data fiduciary / processor status determination	DPDPA 2023, s 2(i)	Determines purpose and means = fiduciary; processes on instructions = processor	**High**	Map each entity in AI value chain; assign fiduciary or processor status; draft Data Processing Agreements
Significant Data Fiduciary (SDF) obligations	DPDPA 2023, s 10	Government notification criteria: data volume, sensitivity, national security, public order	**High**	Monitor SDF designation notifications; if designated: appoint DPO, conduct DPIA, engage independent data auditor annually
Data Principal rights fulfilment — information, correction, erasure	DPDPA 2023, s 12	Response within prescribed period (rules pending); erasure on consent withdrawal	**High**	Build rights management portal; design erasure procedure for AI-trained data; document technical constraints and mitigations for model unlearning
Children's data protection in AI systems	DPDPA 2023, s 9	Verifiable parental consent; no behavioural monitoring or	**Critical**	Implement age verification; disable behavioural profiling for identified minors; audit

Compliance Obligation	Legal Instrument	Standard / Threshold	Risk Level	Required Action
		targeted advertising for under-18		EdTech/gaming/social AI products quarterly
Cross-border data transfer compliance	DPDPA 2023, s 16	Transfer permitted to non-restricted countries (allowlist model; notification pending)	**Medium**	Map all cross-border AI data flows; monitor allowlist notification; implement transfer impact assessments for sensitive personal data
Security safeguards for AI data processing	DPDPA 2023, s 8(5)	Reasonable security practices proportionate to sensitivity of data processed	**High**	Implement ISO 27001 or equivalent; conduct annual security audits; classify AI data stores by sensitivity; apply proportionate controls
Personal data breach notification	DPDPA 2023, s 8(6)	Notify Data Protection Board and affected data principals in prescribed form	**Critical**	Deploy breach detection in AI pipelines; prepare Board notification templates; conduct breach response simulation exercises annually
Penalty exposure	DPDPA 2023, Schedule I	Up to INR 250 crore for	**Critical**	Maintain DPDPA compliance register; conduct quarterly

Compliance Obligation	Legal Instrument	Standard / Threshold	Risk Level	Required Action
assessment and provisioning		specified breaches		compliance reviews; obtain legal privilege opinion on significant data processing activities

2.9 Practitioner's Checklist: DPDPA Compliance for AI Businesses

i. Map all personal data flows within AI training, validation, and inference pipelines.

ii. Identify data fiduciary / data processor status for each entity in the AI value chain.

iii. Assess whether training datasets were collected with consent meeting the DPDPA Section 6 standard; if not, identify alternative lawful grounds or curate new datasets.

iv. Implement a consent management system covering AI-specific data uses, including training, profiling, and automated decision-making.

v. Review whether SDF designation triggers apply; if so, appoint a DPO and commission a Data Protection Impact Assessment.

vi. Design and implement a data principal rights fulfilment mechanism, including response to erasure requests in the AI context.

vii. Assess cross-border data transfer exposure and prepare for the implementation of the allowlist notification.

viii. Review EdTech, gaming, and social media AI products for compliance with Section 9 children's data obligations.

ix. Prepare a personal data breach response plan consistent with the DPDPA notification requirements.

CHAPTER THREE

The Information Technology Act Framework: Intermediary Liability, Cybersecurity, and AI

3.1 The Information Technology Act, 2000: Overview

The Information Technology Act, 2000 (IT Act) remains the foundational statute governing electronic transactions, computer-related offences, and the regulatory framework for internet intermediaries in India. It predates the emergence of modern AI systems, yet its provisions — particularly Section 79 and the subordinate rules made thereunder — have become the primary regulatory instrument applied to AI-powered digital platforms.[35]

The IT Act was substantially amended in 2008, introducing provisions addressing cybercrime, data protection, and platform liability that remain operative alongside the DPDPA 2023. For AI businesses, the IT Act framework is relevant in three principal dimensions: (i) intermediary liability under Section 79 and the IT Rules 2021; (ii) criminal liability for AI-enabled offences under Sections 43, 66, 66A–66F, and 67; and (iii) cybersecurity obligations under CERT-In Directions and related instruments.

3.2 The Intermediary Safe Harbour and AI Platforms

3.2.1 Section 79: The Safe Harbour Provision

Section 79 of the IT Act confers immunity from liability on "intermediaries" — defined in Section 2(1)(w) as persons who receive, store, or transmit electronic records on behalf of others — for third-party information or data made available or hosted by them. The immunity is conditional: the intermediary must exercise "due diligence" and must not initiate the transmission, select the receiver, or select or modify the information.[36]

For AI platforms — particularly generative AI services, AI-powered social media platforms, and AI-driven search engines — the critical question is whether the AI system's role in generating,

[35]Information Technology Act, 2000, No. 21 of 2000 (India), as amended ("IT Act").

[36]IT Act, s 2(1)(w) (definition of "intermediary").

selecting, curating, or amplifying content takes the platform outside the safe harbour. An AI system that generates original content (as opposed to merely transmitting third-party content) is arguably not an "intermediary" with respect to that generated content.[37]

3.2.2 The Active/Passive Distinction in AI Contexts

The Delhi High Court's decision in Christian Louboutin SAS v. Nakul Bajaj articulated the distinction between "active" and "passive" intermediaries. A "passive" intermediary — one that merely stores or transmits without editorial control — retains the Section 79 safe harbour. An "active" intermediary — one that curates, selects, or participates in the content — loses safe harbour protection.[38]

Christian Louboutin SAS v. Nakul Bajaj	
Citation	(2018) 253 DLT 728
Forum	Delhi High Court
Year	2018

Ratio Decidendi

An intermediary that actively participates in unlawful activity, is aware of specific transactions that are unlawful, and derives financial benefit from such transactions cannot claim the benefit of the safe harbour under Section 79 of the IT Act. The court introduced the concept of the "active intermediary" — one that exercises editorial or curatorial control beyond mere technical hosting — as ineligible for the safe harbour.

Regulatory Significance: AI platforms that use recommendation algorithms, generative content tools, or curated search results are potentially "active intermediaries" to the extent that the AI system exercises editorial-equivalent functions over content. Such platforms must ensure either that their AI functions fall within passive technical functions, or that they have implemented adequate content moderation and due diligence systems.

The implication of the Christian Louboutin analysis for AI platforms is profound. A generative AI chatbot that produces original responses is not transmitting third-party content at all — it is

[37]IT Act, s 79 (intermediary safe harbour from liability).

[38]Christian Louboutin SAS v. Nakul Bajaj, (2018) 253 DLT 728 (Del. HC) (on active versus passive roles and intermediary safe harbour).

the primary author of outputs. A recommendation AI that curates and amplifies third-party content exercises editorial-equivalent functions. Neither sits comfortably within the passive intermediary paradigm that underpins the Section 79 safe harbour.[39]

Shreya Singhal v. Union of India	
Citation	(2015) 5 SCC 1
Forum	Supreme Court of India (Two-Judge Bench)
Year	2015

Ratio Decidendi

Section 66A of the IT Act, which criminalised "grossly offensive" online speech, was struck down as unconstitutional being overbroad and incapable of withstanding Article 19(2) scrutiny. The court held that restrictions on online speech must be precisely targeted at intelligible categories of harm. The takedown mechanism under Section 79(3) was read down to require prior judicial order before an intermediary is required to remove content, except in emergency cases.

Regulatory Significance: The Shreya Singhal proportionality framework governs AI content moderation systems. An AI-driven automated takedown system that removes speech without meeting the Section 79(3) read-down standard — i.e., without a court order or compliance with prescribed legal process — may itself be an unlawful restriction on free speech. AI moderation systems must be designed to be precise, reviewable, and consistent with constitutional speech protections.

3.3 IT Rules 2021: Due Diligence Obligations

3.3.1 Overview of the IT Rules 2021

The Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021 (IT Rules 2021), issued under Section 87 of the IT Act, impose a tiered framework of due diligence obligations on intermediaries. All intermediaries must comply with Rule 3; "significant

social media intermediaries" (SSMIs) with registered users above the threshold prescribed by the Central Government (currently 50 lakh users) face additional obligations under Rule 4.[40]

3.3.2 Rule 3 Due Diligence and AI Systems

Rule 3 requires intermediaries to publish terms of service and privacy policies, to inform users of prohibited content categories, to take down content upon receipt of a court order or government direction, to provide a grievance mechanism, and to appoint a Grievance Officer. For AI platforms, Rule 3's prohibition on hosting content relating to threats to national security, public order, and dignity of women has direct implications for content moderation AI systems.[41]

An AI platform that deploys a generative model must ensure that the model's output controls are calibrated to prevent the generation of content in prohibited categories. The deployment of such controls is itself a compliance obligation, not merely a product design choice.

3.3.3 SSMI Obligations and AI Accountability

Rule 4 imposes additional obligations on SSMIs, including (i) appointment of a Chief Compliance Officer, Nodal Contact Person, and Resident Grievance Officer; (ii) publication of monthly compliance reports; and (iii) the implementation of a "traceability" mechanism enabling identification of the originator of information on end-to-end encrypted platforms. The traceability obligation (Rule 4(4)) has faced constitutional challenge on grounds of breach of the right to privacy.[42]

For AI businesses that qualify as SSMIs, the Rule 4 compliance framework requires specific governance structures. The monthly compliance reports must disclose the number of grievances received and actioned, the number of content takedowns, and the use of automated tools for proactive content moderation. AI-driven moderation systems deployed by SSMIs must therefore generate auditable records of automated decisions.[43]

3.4 MeitY Advisory on AI: The March 2024 Framework

[40]Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021 (IT Rules 2021) (as amended 2023).

[41]IT Rules 2021, Rule 3 (due diligence obligations of intermediaries).

[42]IT Rules 2021, Rule 4 (additional obligations for significant social media intermediaries).

On 1 March 2024, MeitY issued an Advisory addressed to "intermediaries and platforms" deploying AI tools, requiring that AI systems deployed on the internet that could potentially be used for disinformation, deep fakes, or generation of unlawful content must (i) obtain prior government approval before deployment; (ii) ensure that outputs do not permit the generation of unlawful content; and (iii) label AI-generated content so as to inform users that the content was produced by an AI system. The Advisory was subsequently clarified on 15 March 2024 to limit its application to certain categories of platforms.[44]

MeitY — Advisory for Intermediaries and Platforms on Use of AI (2024 (1 March & 15 March))

AI platforms and intermediaries must: (i) label AI-generated content to inform users; (ii) ensure AI systems do not permit generation of content unlawful under Indian law; (iii) seek prior government permission before deploying AI systems capable of generating deepfakes or disinformation at scale; (iv) implement "bias removal" mechanisms to ensure AI outputs do not perpetuate unlawful discrimination. Note: As a MeitY advisory, the legal enforceability of these requirements is contested; they are best understood as binding on government-facing platforms and as anticipated regulatory standards for others.

3.5 CERT-In Directions: AI and Cybersecurity Obligations

The CERT-In Directions of April 2022, issued under Section 70B(6) of the IT Act, impose mandatory cybersecurity incident reporting obligations on a broad class of entities including service providers, intermediaries, data centres, and government entities. AI businesses operating as intermediaries, cloud providers, or data processing platforms are within scope.[45]

The Directions require that cybersecurity incidents be reported to CERT-In within six hours of becoming aware of them. For AI systems, this obligation is particularly acute: adversarial attacks on AI models, data poisoning incidents, model inversion attacks, and prompt injection exploits that compromise system integrity are cybersecurity incidents triggering the reporting obligation.

[44]MeitY, Advisory for Intermediaries and Platforms on Use of AI (1 March 2024); Clarification (15 March 2024).

[45]CERT-In, Directions under Section 70B(6) of the IT Act, 2000 (No. 20(3)/2022-CERT-In, 28 April 2022) (the "CERT-In Directions").

AI businesses must additionally maintain logs of ICT systems and applications for 180 days and provide these to CERT-In on demand. The mandatory synchronisation of system clocks with National Physical Laboratory servers applies to all affected entities.

3.5.1 AI-Specific Cybersecurity Threats and Legal Obligations

The deployment of AI systems introduces a class of cybersecurity threats not contemplated in pre-AI regulatory instruments. These include: (i) adversarial attacks — inputs designed to cause AI systems to produce incorrect or harmful outputs; (ii) model inversion — techniques enabling attackers to reconstruct training data from model parameters; (iii) prompt injection — manipulation of large language model inputs to override safety controls; and (iv) data poisoning — contamination of training datasets to corrupt model behaviour.

None of these attack types is expressly addressed in current Indian cybersecurity law. However, the CERT-In Directions' broad definition of "cyber incidents" — which includes "attacks on information technology infrastructure" — is wide enough to capture adversarial attacks, prompt injection, and data poisoning incidents. Practitioners advising AI businesses should ensure that incident response plans specifically address these AI-specific threat vectors.

3.6 Computer-Related Offences and AI

3.6.1 Section 43 and AI Data Damage

Section 43 of the IT Act imposes civil liability for damage to computer systems, computer networks, or data without authorisation. The provision is relevant to AI businesses both as potential victims (where AI systems are attacked) and as potential wrongdoers (where AI systems are used to access or damage third-party data).[46]

3.6.2 Section 66 Offences and AI-Enabled Cybercrime

Section 66 criminalises dishonest or fraudulent computer-related acts causing wrongful gain or loss. Section 66C criminalises identity theft using a computer resource. Section 66E criminalises the capturing or transmission of images of private areas without consent. Each of these provisions is applicable to AI systems used to generate deepfake identities (Section 66C), produce non-

[46] IT Act, s 43A (compensation for failure to protect sensitive personal data or information).

consensual intimate imagery through AI generation (Section 66E), or carry out AI-assisted fraud (Section 66).[47]

Tehseen Poonawalla v. Union of India	
Citation	(2018) 9 SCC 501
Forum	Supreme Court of India
Year	2018

Ratio Decidendi

The State bears a positive obligation to take preventive and remedial action to prevent the spread of mob violence incitement through digital platforms. Platforms must take immediate action upon being notified of content capable of inciting violence. The court issued directions requiring the government to devise guidelines for preventing the dissemination of incendiary content on digital platforms.

Regulatory Significance: Extends platform liability in the context of AI-generated disinformation capable of inciting violence. AI content moderation systems have a heightened obligation to detect and remove content that may trigger mob violence or communal harm, and platforms deploying AI content generation tools bear responsibility for the foreseeable harms from outputs.

3.7 Deepfakes, Synthetic Media, and Legal Liability

Deepfake technology — AI systems that generate synthetic video, audio, or imagery depicting real persons in fabricated scenarios — presents one of the most acute legal challenges in Indian AI law. India does not yet have deepfake-specific legislation, though the MeitY Advisory and Rules 2021 provide partial regulatory coverage.

The legal framework applicable to deepfakes draws from multiple sources: (i) IT Act Section 66E (violation of privacy through transmission of images of private areas — applicable to non-consensual intimate deepfakes); (ii) IT Act Section 67 (obscene electronic content); (iii) IT Act Section 66C (identity theft — applicable to deepfakes used to impersonate); (iv) IPC Section 499 (defamation — applicable to deepfakes portraying real persons in false scenarios); and (v) the

[47] IT Act, s 66 (computer-related offences).

DPDPA 2023 (applicable where the deepfake processing involves the biometric data of identifiable individuals).

For AI businesses whose platforms permit users to create or distribute deepfakes, the combination of Rule 3 prohibited content obligations (IT Rules 2021), the Section 79 safe harbour limitations in respect of AI-generated content, and the DPDPA obligations regarding biometric data processing creates a complex web of compliance requirements.

3.9 Compliance Matrix: IT Act, Intermediary Liability, and Cybersecurity

The following compliance matrix sets out the key obligations, applicable legal instruments, required standards, risk classifications, and mandatory actions for entities operating in this regulatory domain:

Compliance Obligation	Legal Instrument	Standard / Threshold	Risk Level	Required Action
Intermediary status assessment and safe harbour maintenance	IT Act, s 79; IT Rules 2021, Rule 3	Due diligence maintained; no editorial control over third-party content	**High**	Conduct active/passive intermediary analysis for each AI function; document basis for safe harbour claim; do not editorially curate third-party content without safe harbour review
Significant Social Media Intermediary (SSMI) governance	IT Rules 2021, Rule 4	>50 lakh registered users; 36-hour takedown; traceability (if applicable)	**High**	Appoint CCO, NCO, RGO in India; publish monthly compliance reports disclosing AI moderation statistics;

Compliance Obligation	Legal Instrument	Standard / Threshold	Risk Level	Required Action
				implement grievance portal
MeitY Advisory: AI content labelling	MeitY Advisory (March 2024)	All AI-generated content to be labelled as AI-generated	**High**	Implement AI content watermarking or labelling in all generative AI outputs; update T&Cs to disclose AI generation
MeitY Advisory: Unlawful content filters	MeitY Advisory (March 2024); IT Act s 79(3)	AI systems must not permit generation of content unlawful under Indian law	**Critical**	Deploy and maintain AI safety classifiers; conduct red-team testing against Indian law prohibited content categories; document classifier performance
CERT-In cybersecurity incident reporting	CERT-In Directions (April 2022); IT Act s 70B	Report within 6 hours of becoming aware; log retention 180 days	**Critical**	Build AI-specific incident response procedures; classify adversarial attacks, prompt injection, and data poisoning as reportable incidents; appoint CERT-In liaison officer

Compliance Obligation	Legal Instrument	Standard / Threshold	Risk Level	Required Action
Deepfake and synthetic media policy	IT Act ss 66C, 66E, 67; BNS s 356	Prohibition on non-consensual synthetic intimate imagery; identity theft; defamatory deepfakes	**Critical**	Implement deepfake detection in upload/generation pipelines; publish clear deepfake policy; establish expedited takedown for non-consensual deepfakes
Bias removal in AI platform outputs	MeitY Advisory (March 2024); Art. 14, Constitution	AI outputs must not perpetuate unlawful discrimination	**High**	Conduct algorithmic bias audits against protected characteristics; implement bias mitigation in model training and fine-tuning; document results
Log retention and auditability	CERT-In Directions; IT Rules 2021, Rule 3(1)(j)	180-day log retention; logs available to government on demand	**Medium**	Implement automated log archiving for all AI system events; ensure logs are tamper-evident; test production retrieval procedures

3.8 Practitioner's Checklist: IT Act Compliance for AI Businesses

i. Assess whether the AI platform qualifies as an "intermediary" under Section 2(1)(w) and whether the active/passive distinction affects safe harbour eligibility for AI-generated content.

ii. If an SSMI, implement the full Rule 4 governance structure: CCO, NCO, RGO, monthly compliance reports, and AI content moderation disclosure.

iii. Review MeitY Advisory compliance: content labelling, unlawful content filters, bias removal mechanisms.

iv. Implement CERT-In Directions: incident reporting within 6 hours, 180-day log retention, NTP server synchronisation.

v. Develop AI-specific cybersecurity threat models covering adversarial attacks, prompt injection, model inversion, and data poisoning.

vi. Review deepfake and synthetic media policies for compliance with Section 66C, 66E, and 67, and ensure content moderation AI is trained to detect such content.

vii. Ensure AI output labelling is consistent with MeitY Advisory requirements.

CHAPTER FOUR

SEBI's Regulatory Framework for Artificial Intelligence in Capital Markets

4.1 Introduction: AI and the Indian Capital Markets

Artificial intelligence and machine learning have penetrated the Indian capital markets at multiple levels: high-frequency and algorithmic trading systems, robo-advisory platforms providing personalised investment recommendations, AI-driven research analytics, fraud and market manipulation surveillance, and risk management systems deployed by exchanges and clearing corporations. SEBI's regulatory response has been progressive and technically sophisticated, though it remains anchored in a framework designed primarily for algorithmic trading rather than AI systems in the full contemporary sense.[48]

This chapter surveys SEBI's regulatory architecture for AI in capital markets, analyses the key circulars and guidelines, extracts the applicable legal principles from tribunal and court decisions, and identifies the principal compliance obligations for market participants deploying AI systems.

SEBI — Circular on AI/ML Applications by Registered Intermediaries (2019 (No. SEBI/HO/MIRSD/TPD/CIR/P/2019/135))

Requires SEBI-registered intermediaries deploying AI/ML applications to: (i) establish a comprehensive risk management framework; (ii) ensure explainability of AI/ML outputs; (iii) maintain audit trails; (iv) conduct regular back-testing and stress testing; (v) implement ethical AI principles including fairness and transparency; (vi) have board-level accountability for AI/ML adoption. Defines AI/ML broadly to encompass all systems using statistical learning techniques to generate investment decisions or recommendations.

4.2 SEBI's Jurisdiction over AI in Capital Markets

[48]SEBI, "Circular on Usage of Artificial Intelligence and Machine Learning Applications by SEBI Registered Intermediaries" (Circular No. SEBI/HO/MIRSD/TPD/CIR/P/2019/135, 4 November 2019) (hereinafter "SEBI AI/ML Circular 2019").

SEBI's jurisdiction over AI in capital markets derives from Section 11 of the SEBI Act, which empowers SEBI to protect the interests of investors and to promote the development and regulation of securities markets. Specifically, SEBI's power to issue directions and circulars to "stock exchanges, mutual funds, other persons associated with the securities market" is the legal basis for its AI/ML circulars.[49]

The scope of SEBI's regulatory authority extends to: (i) registered intermediaries including stock brokers, sub-brokers, portfolio managers, investment advisers, research analysts, and mutual funds; (ii) market infrastructure institutions including stock exchanges, depositories, and clearing corporations; and (iii) listed companies to the extent they deploy AI in investor-facing communications or market-sensitive disclosures.

4.3 Algorithmic Trading Framework: The Foundation

4.3.1 SEBI's 2012 Algo Trading Circular

SEBI's foundational regulatory instrument for AI in markets is the 2012 Circular on Algorithmic Trading, which established the basic framework: exchange-level approval for algorithmic strategies, mandatory audit trails, risk controls including maximum order-per-second limits, and broker liability for all orders placed through algorithmic systems.[50]

This framework predates modern AI/ML systems, but its core principles — approval before deployment, audit trail maintenance, broker accountability, and risk controls — have been carried forward and adapted in subsequent instruments to encompass AI-powered trading.

4.3.2 Kill-Switch and Circuit Breaker Requirements

A central compliance obligation for AI trading systems is the mandatory implementation of "kill switches" — controls enabling immediate cessation of algorithmic trading activity in case of system anomaly or market disruption. The Technical Advisory Committee Report of July 2022 recommended enhanced kill-switch requirements specifically for AI/ML-based trading systems, recognising that the speed and autonomous character of such systems creates systemic risk.[51]

[49]SEBI Act, s 11 (SEBI's power to issue circulars and directions for investor protection and market development).

[50]SEBI, "Circular on Algorithmic Trading" (CIR/MRD/DP/09/2012, 30 March 2012).

[51]SEBI, "Report of the Technical Advisory Committee on Algo Trading" (July 2022) (recommending enhanced audit trails and kill-switch requirements for algorithmic trading systems including AI/ML-based systems).

4.3.3 The NSE Co-location Case and Systemic Risk from AI Trading

The NSE Co-location Case — one of the most significant enforcement actions in Indian capital markets history — arose from structural inequities in co-location infrastructure that gave certain algorithmic (and later AI-driven) trading participants preferential data access. The case illustrates the systemic risk dimension of AI in high-frequency trading and the governance failures that can emerge.[52]

In re: National Stock Exchange of India Ltd.	
Citation	WTM/GM/EFD/DRAIII/40/2019
Forum	SEBI Whole-Time Member Order
Year	2019

Ratio Decidendi

The NSE and certain officials were found to have permitted structural information asymmetry in co-location infrastructure, enabling certain brokers to gain first-mover advantage in order matching queues. The Order held that a market infrastructure institution has a fiduciary duty to ensure fair, equitable access to all market participants and that any infrastructure design — whether technical, algorithmic, or AI-driven — that creates structural unfairness violates the SEBI Act's investor protection mandate.

Regulatory Significance: Establishes that AI and algorithmic trading infrastructure must be designed to preserve market fairness. AI systems deployed by exchanges or trading participants that create structural information advantages may violate SEBI's investor protection mandate, regardless of technical sophistication. Governance frameworks for AI in capital markets must include fairness-by-design requirements.

4.4 AI/ML Circular 2019: Core Obligations

4.4.1 Risk Management Framework

The SEBI AI/ML Circular 2019 requires registered intermediaries to establish a "comprehensive risk management framework" for AI/ML applications. This framework must address: (i) pre-

[52]NSE-SEBI Co-location Case; In re: National Stock Exchange of India Ltd., WTM/GM/EFD/DRAIII/40/2019 (SEBI, 11 February 2019) (structural and governance failures in co-location infrastructure of direct relevance to high-frequency AI trading).

deployment validation including back-testing against historical data; (ii) stress testing against adverse market scenarios; (iii) continuous model performance monitoring; (iv) model drift detection; and (v) periodic re-validation and re-approval of AI/ML models.[53]

Model drift — the degradation of AI model performance over time as market conditions evolve — is a critical risk in financial AI applications. An AI credit scoring model, a high-frequency trading algorithm, or a fraud detection system trained on historical data may perform poorly in novel market conditions. The Circular's requirement of continuous monitoring and periodic re-validation addresses this risk.

4.4.2 Explainability Requirements

The Circular requires that AI/ML outputs be "explainable" — that the reasoning behind AI-generated investment decisions or recommendations be capable of being understood and communicated. This requirement creates a de facto prohibition on "black box" AI systems whose internal logic cannot be interrogated or articulated. It is a significant constraint on the deployment of deep learning systems, which are inherently less interpretable than rule-based or linear models.[54]

Practitioners advising intermediaries deploying deep neural networks for trading or advisory functions must ensure that explainability mechanisms — such as attention visualisation, SHAP values, or counterfactual explanations — are integrated into the AI system and that outputs can be translated into humanly comprehensible decision rationales.

4.4.3 Board-Level Accountability

The Circular imposes board-level responsibility for AI/ML adoption. The board of a registered intermediary must formally approve the AI/ML strategy, receive periodic reports on AI/ML performance, and ensure that adequate governance mechanisms are in place. This requirement aligns AI governance with the general corporate governance standards applicable to listed companies and regulated financial entities.[55]

4.5 Robo-Advisory Services: Regulatory Framework

4.5.1 SEBI (Investment Advisers) Regulations 2013 and AI Advisory

Robo-advisory services — AI systems that provide automated, personalised investment advice — are subject to SEBI (Investment Advisers) Regulations, 2013. An entity providing robo-advisory services is an "investment adviser" within the meaning of the Regulations, and must be registered with SEBI.[56]

SEBI's 2022 Consultation Paper on Governance of Robo Advisory Services proposed requirements including: (i) disclosure of the AI nature of advice; (ii) profiling of client risk appetite through AI-validated questionnaires; (iii) suitability obligations ensuring AI recommendations are appropriate for the specific client; (iv) human oversight of AI recommendations before delivery to high-risk client profiles; and (v) grievance mechanisms specific to AI advisory outputs.[57]

4.5.2 Suitability and Fiduciary Obligations in AI Advisory

The fundamental challenge in AI advisory regulation is ensuring that the AI system's personalisation of advice satisfies the suitability and fiduciary obligations that apply to human advisers. An AI system that recommends a high-volatility instrument to a risk-averse client profile or fails to account for concentrated exposure in a client's existing portfolio has failed its suitability obligation.

The fiduciary standard applicable to investment advisers — the obligation to act in the best interests of the client — must be programmed into the AI system's objective function. A recommendation AI optimised for revenue or commissions rather than client outcomes fails this standard, irrespective of technical sophistication.

4.6 Insider Trading and AI Systems

The deployment of AI systems in securities trading raises distinct insider trading concerns. Where an AI system has access to unpublished price-sensitive information (UPSI) — whether through employee access to corporate databases, through algorithmic processing of corporate

[56]SEBI (Investment Advisers) Regulations, 2013 (as amended); SEBI, "Circular on Investment Adviser Regulations" (February 2020).
[57]SEBI, "Consultation Paper on Governance of Robo Advisory Services" (September 2022).

disclosures before public dissemination, or through inclusion of UPSI-containing documents in training datasets — the system may be deemed to be "in possession of UPSI" within the meaning of the SEBI (Prohibition of Insider Trading) Regulations, 2015.[58]

The legal analysis must address whether an AI system can be deemed to "possess" information, whether the entity operating the AI system is deemed to be in possession of UPSI fed to the system, and whether trading decisions generated by an AI system with UPSI exposure constitute insider trading. The regulatory position remains unsettled, but the conservative compliance approach requires treating AI systems as "insiders" where they have access to UPSI.

SEBI v. Kishore R. Ajmera	
Citation	(2016) 6 SCC 368
Forum	Supreme Court of India
Year	2016

Ratio Decidendi

SEBI can infer the presence of market manipulation from patterns of trading activity even in the absence of direct evidence of a fraudulent scheme. Where trading patterns are inconsistent with legitimate investment behaviour and are accompanied by consequential price or volume effects, an inference of manipulation is permissible. The court affirmed SEBI's power to draw evidentiary inferences from algorithmic data.

Regulatory Significance: Directly applicable to AI-driven market manipulation detection. SEBI's AI-powered surveillance systems that detect anomalous trading patterns consistent with manipulation may serve as the basis for enforcement proceedings, even in the absence of direct evidence. Conversely, registered intermediaries must ensure that their own AI trading systems cannot be characterised as generating manipulative patterns.

4.7 SEBI's AI Surveillance Framework

SEBI has deployed its own AI and ML systems for market surveillance, including systems designed to detect insider trading, market manipulation, front-running, and wash trading. The

[58]SEBI (Prohibition of Insider Trading) Regulations, 2015, Reg. 4 (communication and trading by insiders); applicable to AI systems with access to UPSI.

Integrated Market Surveillance System (IMSS) and its successors use AI to process real-time trading data and flag anomalous activity for enforcement review.

The deployment of AI in regulatory surveillance raises fairness concerns: if the regulatory AI system generates false positives, regulated entities face the burden of disproving algorithmically generated allegations. Practitioners must be prepared to challenge the evidentiary weight of AI-generated surveillance outputs in SAT proceedings.

4.9 Compliance Matrix: SEBI Regulation of AI in Capital Markets

The following compliance matrix sets out the key obligations, applicable legal instruments, required standards, risk classifications, and mandatory actions for entities operating in this regulatory domain:

Compliance Obligation	Legal Instrument	Standard / Threshold	Risk Level	Required Action
Exchange/SEBI approval for AI/ML algorithmic strategies	SEBI Algo Trading Circular (2012); Master Circular 2024 Ch.15	Prior approval before live deployment of any new AI trading algorithm	**Critical**	Submit new AI strategy for exchange approval; maintain approval register; re-apply on material model change
AI/ML Risk Management Framework	SEBI AI/ML Circular 2019 (No. SEBI/HO/MIRSD/TPD/CIR/P/2019/135)	Back-testing, stress testing, continuous monitoring, drift detection	**High**	Establish documented MRM framework; conduct quarterly

Compliance Obligation	Legal Instrument	Standard / Threshold	Risk Level	Required Action
				back-testing; document stress test results; implement automated drift alerts
Kill-switch and circuit breaker for AI trading	SEBI Algo Trading Framework; TAC Report 2022	Immediate cessation capability; tested and operational at all times	**Critical**	Test kill-switch monthly; document kill-switch architecture; ensure kill-switch is reachable independently of AI system operation
Explainability of AI/ML investment decisions	SEBI AI/ML Circular 2019	Outputs must be explainable; reasoning communicable to compliance and regulators	**High**	Integrate SHAP, LIME, or equivalent explainability tools; maintain decision logs with explanation records; train

Compliance Obligation	Legal Instrument	Standard / Threshold	Risk Level	Required Action
				compliance staff on model output interpretation
Board-level AI governance and reporting	SEBI AI/ML Circular 2019	Board approval of AI strategy; periodic performance reports to board	**High**	Table AI governance policy for board approval; implement quarterly AI board reports covering performance, risk events, and regulatory developments
Investment Adviser registration for robo-advisory	SEBI (IA) Regulations 2013; Consultation Paper 2022	Registration mandatory; suitability, disclosure, and fiduciary obligations	**Critical**	Register robo-advisory platform as IA; implement AI-driven suitability assessment; disclose AI nature of advice; maintain

Compliance Obligation	Legal Instrument	Standard / Threshold	Risk Level	Required Action
				human escalation for complex/high-risk profiles
Insider trading compliance for AI systems with UPSI access	SEBI (PIT) Regulations 2015, Reg. 4	AI systems with UPSI access treated as insiders; trading restrictions apply	**Critical**	Map all AI systems with potential UPSI exposure; implement information barriers; restrict trading through UPSI-exposed systems; maintain UPSI access register
Audit trail maintenance for AI trading decisions	SEBI Algo Trading Framework; Master Circular 2024	Complete audit trail of all AI-generated orders; 5-year retention	**High**	Implement immutable audit logging of all AI order generation events; include model version, input features, and

Compliance Obligation	Legal Instrument	Standard / Threshold	Risk Level	Required Action
				output with each log record

4.8 Practitioner's Checklist: SEBI Compliance for AI in Capital Markets

(a) Obtain exchange/SEBI approval before deploying new AI/ML-based algorithmic trading strategies.

(b) Implement the AI/ML risk management framework: back-testing, stress testing, continuous monitoring, model drift detection.

(c) Ensure AI trading systems have kill-switch and circuit breaker controls that comply with SEBI's technical specifications.

(d) Implement explainability mechanisms for all AI/ML-generated investment decisions or recommendations.

(e) Secure board-level approval and periodic reporting for AI/ML adoption in accordance with the 2019 Circular.

(f) Register robo-advisory platforms as investment advisers; implement suitability, disclosure, and fiduciary compliance for AI advisory systems.

(g) Review AI systems with access to UPSI for insider trading compliance; implement information barriers and access controls.

(h) Maintain comprehensive audit trails for all AI-generated trading decisions for a minimum of five years.

CHAPTER FIVE
RBI's Regulatory Framework for AI in Banking, Lending, and Payments

5.1 Introduction: AI in Indian Banking

The deployment of artificial intelligence in the Indian banking and financial services sector has been rapid and pervasive. AI systems are now deployed in credit underwriting and scoring, know-your-customer (KYC) verification, anti-money laundering (AML) transaction monitoring, fraud detection, customer service chatbots, collections management, and treasury operations. The Reserve Bank of India (RBI), exercising its powers under the RBI Act, the Banking Regulation Act, and the Payment and Settlement Systems Act, has progressively developed a regulatory framework addressing these deployments.[59]

The RBI's approach is characterised by principle-based regulation: rather than prescribing specific technical architectures, it establishes outcome-based standards — explainability, fairness, accountability, robustness — and leaves regulated entities to determine how to achieve those outcomes. This approach is consistent with international regulatory practice in the financial sector and with the BCBS principles on AI in banking issued by the Basel Committee.

RBI —Master Direction on IT Governance, Risk, Controls and Assurance Practices (2023)

Requires regulated entities (REs) to establish an AI/ML Governance Framework covering: (i) risk assessment before deployment; (ii) model validation by independent internal or external reviewers; (iii) explainability and bias testing; (iv) continuous performance monitoring and model drift detection; (v) escalation protocols for model failures; (vi) board-level AI oversight through the IT Strategy Committee. Defines AI/ML as including all systems using statistical or machine learning techniques to generate decisions or recommendations. Applies to banks, NBFCs, and payment system operators.

[59]Reserve Bank of India Act, 1934, No. 2 of 1934 (India) (hereinafter "RBI Act"); Banking Regulation Act, 1949, No. 10 of 1949 (India).

5.2 RBI's AI Governance Framework

5.2.1 IT Governance and AI

The Draft Master Direction on IT Governance of November 2023 is the most comprehensive RBI instrument specifically addressing AI. It requires regulated entities to establish an "AI/ML Governance Framework" as a component of the broader IT governance architecture. Key requirements include independent model validation, explainability testing, bias assessment, and board-level oversight.[60]

The requirement of independent model validation is particularly significant. It mandates that AI/ML models used in credit decisioning, risk management, and customer-facing applications be validated by a team independent of the model development team — either internally or through external audit. This requirement is designed to prevent the deployment of flawed or biased models into production without independent verification.

5.2.2 Model Risk Management

The RBI's approach to model risk management draws on the Basel Committee's SR 11-7 guidance (US Federal Reserve) and the EBA's guidelines on internal models, adapted for the Indian context. Model risk — the risk of loss arising from incorrect or inappropriate use of AI/ML models — must be managed through a Model Risk Management (MRM) framework covering model identification, model documentation, validation, approval, and ongoing monitoring.[61]

Regulated entities must maintain a model inventory cataloguing all AI/ML models in production, including purpose, data inputs, output types, validation status, and performance metrics. The model inventory must be reviewed at least annually and updated following any material model change.

5.3 Digital Lending and AI Credit Decisioning

5.3.1 Digital Lending Guidelines 2022

[60]RBI, "Draft Master Direction – Information Technology Governance, Risk, Controls and Assurance Practices" (November 2023) (hereinafter "RBI IT Governance Draft").

[61]RBI, "Circular on Risk-Based Internal Audit" (DoS.CO.PPG./SEC.04/11.01.005/2019-20, 9 March 2020) (requiring AI-based risk assessment tools to be subject to independent audit).

The RBI's Digital Lending Guidelines of September 2022 establish the regulatory framework applicable to AI-powered digital lending platforms. The Guidelines were issued in response to the proliferation of unregulated digital lending apps using AI credit scoring to extend high-interest consumer credit without adequate disclosures or borrower protections.[62]

RBI — Circular on Digital Lending Guidelines (2022 (DOR.CRE.REC.66/21.07.001/2022-23))

Key requirements for AI-based digital lending: (i) disclosure of AI/algorithm-based credit decision criteria in plain language; (ii) prohibition on shadow operations — all lending activity must flow through regulated entities; (iii) Key Fact Statement (KFS) mandatory before loan disbursement; (iv) data collected by lending apps limited to need-based data with explicit borrower consent; (v) prohibition on access to mobile phone resources (contacts, call logs) for credit scoring without explicit disclosure; (vi) standardised grievance redressal including review of AI credit denial.

5.3.2 Fairness in AI Credit Scoring

The RBI's Fair Practices Code for Lenders requires that credit decisions be communicated to applicants with reasons, and that borrowers have a right to seek review. Applied to AI credit scoring, this requirement mandates that where an AI system generates a credit denial or adverse credit terms, the regulated entity must communicate the reasons for the decision in terms that the borrower can understand.[63]

This "adverse action notice" obligation — well-established in US and EU credit law — is an emerging standard in Indian banking regulation. The explainability requirement in the IT Governance Draft complements this: if an AI credit scoring model cannot generate human-comprehensible explanations for its outputs, it cannot satisfy the Fair Practices Code adverse action notice obligation.

An additional concern is demographic bias in AI credit scoring. Models trained on historical data may perpetuate or amplify existing credit access disparities along lines of gender, caste, religion,

[62]RBI, "Circular on Digital Lending Guidelines" (DOR.CRE.REC.66/21.07.001/2022-23, 2 September 2022) (hereinafter "Digital Lending Circular 2022").

[63]RBI, "Fair Practices Code for Lenders" (2003, updated periodically) (applicable to AI credit scoring decisions).

or geography. The RBI's requirement of bias testing is designed to detect and remediate such disparities before they translate into discriminatory lending outcomes.

State Bank of India v. Rajendra Kumar Sharma	
Citation	(2014) 9 SCC 287
Forum	Supreme Court of India
Year	2014

Ratio Decidendi

A financial institution owes a duty of care to customers in the operation of automated systems processing financial transactions. Where an automated system generates an error causing financial loss to a customer, the institution cannot disclaim liability by reference to the automated nature of the transaction. The duty of care of a financial institution is non-delegable to automated systems.

Regulatory Significance: Foundational authority for regulated entities' non-delegable liability for AI credit decisions. A bank cannot escape liability for a discriminatory, erroneous, or biased AI credit decision by attributing the outcome to the algorithm. Board-level accountability for AI, as required by the RBI IT Governance Draft, follows logically from this principle.

5.4 KYC/AML and AI Systems

5.4.1 AI-Assisted KYC

The RBI's KYC Master Circular permits regulated entities to use AI/ML-assisted KYC tools, including video-based customer identification processes (V-CIP), document verification using optical character recognition, and biometric authentication. AI systems used for KYC must comply with the technical specifications issued by the RBI for each permitted KYC method.[64]

A key compliance concern in AI-assisted KYC is the accuracy and bias performance of AI document recognition and face matching systems across demographic groups. AI facial recognition systems have been found to exhibit higher error rates for women and darker-skinned

[64]RBI, "Master Circular on Know Your Customer (KYC) Norms/Anti-Money Laundering (AML) Standards" (updated July 2024) (on AI-assisted KYC and AML compliance).

individuals. Regulated entities deploying AI facial recognition for KYC must conduct bias testing across demographic subgroups and must not deploy systems with materially different error rates across protected groups.

5.4.2 AI-Powered AML Transaction Monitoring

AI transaction monitoring systems have largely supplanted rule-based AML systems in large Indian banks. These systems analyse transaction patterns to detect structuring, layering, and integration activity consistent with money laundering and terrorist financing. The RBI KYC Master Circular requires that transaction monitoring systems be capable of generating suspicious transaction reports (STRs) meeting the standards required by the Financial Intelligence Unit-India (FIU-IND).[65]

AI AML systems present specific compliance challenges: false positive rates (legitimate transactions flagged as suspicious) generate significant compliance costs and may affect customer experience; false negatives (actual suspicious transactions not detected) create regulatory exposure. Regulated entities must calibrate their AI AML systems to achieve acceptable performance on both dimensions, and must document the calibration methodology for regulatory inspection.

5.5 Payments AI and the PSS Act Framework

The Payment and Settlement Systems Act, 2007 (PSS Act) governs payment system operators in India, including entities deploying AI in payment processing, fraud detection, and customer authentication. AI systems used for fraud detection in payment systems must be authorised components of the payment system's operational architecture as notified to the RBI.[66]

The UPI system, operated by NPCI, increasingly relies on AI-powered fraud detection that analyses transaction metadata, device fingerprints, and behavioural patterns to detect fraudulent transactions in real time. Participants in the UPI ecosystem — banks, payment aggregators, and third-party application providers — must ensure that their AI fraud detection components are consistent with NPCI's technical standards and the RBI's payment system regulations.

[66]Payment and Settlement Systems Act, 2007, No. 51 of 2007 (India) (governing AI in payment systems).

5.5.1 RBI Regulatory Sandbox and AI FinTech

The RBI's Regulatory Sandbox framework enables fintech companies, including AI-driven lenders, payment processors, and robo-advisers, to test their products in a controlled environment under relaxed regulatory conditions. The Sandbox has included AI-focused cohorts, recognising that AI-driven financial products may require operational testing in live market conditions to assess regulatory compliance before full deployment.[67]

5.6 Compliance Matrix: RBI Regulation of AI in Banking and Payments

The following compliance matrix sets out the key obligations, applicable legal instruments, required standards, risk classifications, and mandatory actions for entities operating in this regulatory domain:

Compliance Obligation	Legal Instrument	Standard / Threshold	Risk Level	Required Action
AI/ML Governance Framework — board-level adoption	RBI IT Governance Draft 2023; Banking Regulation Act s 10B	Board-approved framework covering model lifecycle, validation, oversight	**Critical**	Constitute IT Strategy Committee with AI sub-committee; table AI governance policy for board approval; review annually
Independent model validation	RBI IT Governance Draft 2023	Validation by team independent of model development; before production deployment	**High**	Establish independent model validation unit or engage external validator; document validation methodology and results; maintain

[67] RBI, "Master Direction – Reserve Bank of India (Regulatory Sandbox) Directions, 2019" (as amended 2021).

Compliance Obligation	Legal Instrument	Standard / Threshold	Risk Level	Required Action
				model validation register
Digital Lending Guidelines — KFS and borrower disclosure	RBI Digital Lending Circular 2022	KFS mandatory before disbursement; AI credit criteria disclosed in plain language	**Critical**	Implement KFS generation in digital lending workflow; audit AI credit denial communications for regulatory compliance; test KFS with diverse borrower profiles
Adverse action notice for AI credit decisions	RBI Fair Practices Code; Digital Lending Circular 2022	Reasons for adverse credit decision communicated to applicant; must be comprehensible	**High**	Integrate explainability module into AI credit scoring system; generate human-readable adverse action notices; maintain notice quality through periodic audits
Demographic bias testing in AI credit and KYC systems	RBI IT Governance Draft 2023; Art. 14, Constitution	No materially different error rates across gender, geography, or protected group	**High**	Conduct annual bias audit across demographic subgroups; document results; remediate identified

Compliance Obligation	Legal Instrument	Standard / Threshold	Risk Level	Required Action
				biases before next deployment cycle
AI AML transaction monitoring calibration	RBI KYC Master Circular; PMLA 2002	STR generation at standards required by FIU-IND; acceptable false positive/negative rates	**Critical**	Document AML model calibration methodology; conduct semi-annual model validation; maintain FIU-IND reporting statistics; alert on performance degradation
Digital lending app data minimisation	RBI Digital Lending Circular 2022; DPDPA 2023 s 8	App data collection limited to need-based; no access to mobile contacts or call logs	**High**	Audit lending app permissions; remove any non-need-based data collection; update app store privacy disclosures to reflect actual data collected
Regulatory Sandbox participation for novel AI products	RBI Regulatory Sandbox Directions 2019 (as amended)	Novel AI financial products tested in Sandbox before full deployment	**Medium**	Assess novel AI products against Sandbox eligibility criteria; prepare Sandbox application where applicable; engage RBI FinTech Department proactively

5.7 Practitioner's Checklist: RBI Compliance for AI in Banking

i. Establish an AI/ML Governance Framework compliant with the RBI IT Governance Draft: model inventory, independent validation, bias testing, board oversight.

ii. Review digital lending operations for compliance with the Digital Lending Guidelines: KFS, borrower consent for data collection, shadow operation prohibition.

iii. Implement adverse action notice capability for all AI credit scoring systems: explainability must be sufficient to generate compliant adverse action communications.

iv. Conduct demographic bias testing on AI KYC facial recognition and credit scoring systems; document results and remediation steps.

v. Calibrate AI AML transaction monitoring systems for acceptable false positive/negative rates; document calibration and validation.

vi. Assess whether novel AI financial products require testing through the RBI Regulatory Sandbox prior to full deployment.

vii. Review AI data collection practices in lending apps for compliance with Digital Lending Guidelines data minimisation requirements.

CHAPTER SIX

Competition Law and Artificial Intelligence: The CCI Framework

6.1 Introduction: AI, Data, and Competition

The intersection of artificial intelligence and competition law has emerged as one of the most consequential areas of regulatory concern in India. AI systems are simultaneously competitive tools — enabling novel products and efficiencies — and potential instruments of market distortion, through algorithmic pricing coordination, data-driven exclusion, and exploitative personalisation. The Competition Commission of India (CCI) has engaged with these concerns through its market studies, enforcement actions, and legislative reforms.[68]

The Competition (Amendment) Act, 2023 significantly strengthened the CCI's toolkit, introducing a deal value threshold for AI acquisitions (addressing the "killer acquisition" problem), strengthening the CCI's power to investigate digital markets, and importing the concept of "significant digital market participant" — signalling an intent to regulate large technology platforms with heightened scrutiny.

6.2 Algorithmic Pricing and Section 3

6.2.1 The Hub-and-Spoke Problem

Section 3 of the Competition Act prohibits agreements between enterprises that cause an appreciable adverse effect on competition. The deployment of common algorithmic pricing tools by multiple competitors raises the "hub-and-spoke" problem: where competitors independently adopt a common AI pricing algorithm supplied by a common vendor, and the algorithm processes competitor pricing signals to arrive at prices, the use of the algorithm may constitute a horizontal agreement within the meaning of Section 3(3).[69]

[68]Competition Act, 2002, No. 12 of 2003 (India) (as amended by Competition (Amendment) Act, 2023) (hereinafter "Competition Act").

[69]Competition Act, s 3 (anti-competitive agreements).

The CCI has not yet addressed algorithmic hub-and-spoke cases directly, but its e-commerce market study and the European Commission's enforcement actions in algorithmic pricing (in the Amazon, Booking.com, and Eturas matters) provide the analytical framework. The key question is whether the common AI pricing tool serves as a "meeting of minds" substituting for explicit horizontal agreement.

6.2.2 Predictive Pricing AI and Section 3(3)

A more acute concern is AI systems that learn to predict and match competitor prices without explicit coordination. Reinforcement learning pricing algorithms that observe market price data and adjust prices to maximise profits may, over time, converge on supra-competitive prices through a process that resembles — without constituting — explicit collusion. The CCI's analytical framework must grapple with whether such "tacit algorithmic collusion" is caught by Section 3(3)'s prohibition of price-fixing agreements.

6.3 Abuse of Dominance and AI Systems

6.3.1 Google Android Case: Algorithmic Bias as Abuse

The CCI's landmark order in the Google Android matter is the most significant Indian authority on the application of competition law to AI-mediated markets. The CCI found that Google had abused its dominant position in the markets for licensable mobile operating systems and Android app distribution.[70]

CCI v. Google LLC (Android Case)	
Citation	Case No. 39 of 2018
Forum	Competition Commission of India
Year	2022
Ratio Decidendi *Google's requirement that original equipment manufacturers (OEMs) pre-install Google Search and Chrome as conditions of accessing the Play Store constituted tying and exclusive*	

[70]CCI v. Google LLC, Case No. 39 of 2018 (CCI Order, 20 October 2022) (hereinafter "Google Android Case") — CCI imposed INR 1,337.76 crore penalty for abuse of dominant position.

dealing in violation of Section 4(2)(a) and (e) of the Competition Act. Google's algorithmic allocation of prime screen real estate to its own products over competing services constituted self-preferencing abuse. A platform operator in a dominant position that uses its algorithmic architecture to advantage its own downstream services over equally or more meritorious competing services engages in an exclusionary abuse.

Regulatory Significance: Foundational Indian authority on algorithmic self-preferencing as abuse of dominance. AI-powered platform operators in dominant positions must ensure that recommendation, ranking, and display algorithms are not designed to favour affiliated services. The case establishes that algorithmic architecture choices are subject to competition law scrutiny.

Matrimony.com Ltd. v. Google LLC	
Citation	Case No. 07 & 30 of 2012
Forum	Competition Commission of India
Year	2018

Ratio Decidendi

Google's algorithmic search result ranking that systematically favoured its own vertical search products over competing generic and vertical search services constituted abuse of its dominant position in the online general search services market. The CCI found that a dominant search operator's algorithmic choices — even those framed as quality improvements — must not have the effect of foreclosing competition from the market.

Regulatory Significance: Establishes that search algorithm design by dominant operators is subject to competition law scrutiny. AI systems that rank or recommend content, products, or services must not be designed to achieve exclusionary effects. The principle applies beyond search to AI recommendation systems in e-commerce, social media, and financial services platforms.

6.3.2 Data as Essential Facility

The intersection of AI with the "essential facility" doctrine is a growing area of competition concern. Where an AI system's competitive effectiveness depends on access to data that is

controlled by a dominant firm and not available to competitors on reasonable terms, the dominant firm's refusal to provide access may constitute an exclusionary abuse.[71]

The CCI has not yet expressly adopted the "essential facility" doctrine for data, but its market studies have recognised that data concentration confers significant competitive advantages in AI markets. Practitioners advising AI companies in AI-data disputes with dominant platforms should consider whether the essential facility doctrine, applied to data, supports a Section 4 complaint.

6.4 Merger Control and AI Acquisitions

The Competition (Amendment) Act, 2023 introduced a deal value threshold of INR 2,000 crore for combinations where the target has substantial business operations in India. This threshold was specifically designed to capture "killer acquisitions" — the purchase of nascent AI startups by large platforms before those startups can develop into competitive threats.[72]

AI acquisitions present distinctive competition concerns beyond conventional asset-based analysis: the competitive significance of an AI acquisition may lie in the target's training data, talent, and model capabilities rather than in its revenue or market share. The CCI's review of AI acquisitions must assess data concentration effects, talent lock-in, and the potential for the acquirer to use the target's AI capabilities to foreclose competition.

6.5 Compliance Matrix: Competition Law and AI (CCI Framework)

The following compliance matrix sets out the key obligations, applicable legal instruments, required standards, risk classifications, and mandatory actions for entities operating in this regulatory domain:

Compliance Obligation	Legal Instrument	Standard / Threshold	Risk Level	Required Action
Algorithmic pricing hub-	Competition Act 2002, s	No horizontal coordination	Critical	Conduct competition law audit of AI pricing

[71]Competition Act, s 4 (abuse of dominant position).

[72]Competition (Amendment) Act, 2023, s 6A (deal value threshold for combinations).

Compliance Obligation	Legal Instrument	Standard / Threshold	Risk Level	Required Action
and-spoke assessment	3(3); CCI v. Google (2022)	through common pricing AI; no competitor signal incorporation		systems; ensure pricing AI does not incorporate competitor pricing as input; document independent pricing rationale
Self-preferencing audit for dominant AI platforms	Competition Act 2002, s 4(2); CCI v. Google (2022)	No algorithmic design favouring affiliated services over equally meritorious competitors	**Critical**	Commission independent algorithmic audit of ranking/recommendation AI; implement fairness metrics; document audit results and remediation steps
Data access and essential facility obligations	Competition Act 2002, s 4(2)(c); Competition Amendment Act 2023	Refusal of data access by dominant firm may constitute exclusionary abuse	**High**	Review data licensing policies; ensure proprietary dataset access terms are not exclusionary; engage CCI proactively if data access disputes arise
Merger control filing for AI acquisitions	Competition Act 2002, s 5; Competition Amendment Act 2023, s 6A	Deal value threshold INR 2,000 crore + substantial Indian operations	**High**	Screen all AI acquisitions against deal value threshold; assess data concentration effects; prepare CCI filing if threshold triggered

Compliance Obligation	Legal Instrument	Standard / Threshold	Risk Level	Required Action
Algorithmic collusion monitoring	Competition Act 2002, s 3(3)	RL pricing AI must not achieve supracompetitive equilibria through tacit coordination	**High**	Monitor RL pricing algorithm outputs for supracompetitive patterns; establish competitive intelligence protocols; consult competition counsel on novel pricing AI deployments
Market study engagement and information cooperation	Competition Act 2002, s 49	Cooperation with CCI market studies and information requests	**Medium**	Designate CCI liaison; monitor market study announcements; respond substantively and timely to information requests

6.6 Practitioner's Checklist: CCI Compliance for AI Businesses

i. Audit algorithmic pricing systems for hub-and-spoke coordination risk; ensure pricing AI does not incorporate competitor pricing signals in ways that could constitute horizontal coordination.

ii. Review recommendation and ranking AI systems operated by dominant platforms for self-preferencing effects; implement algorithmic auditing to detect and prevent exclusionary ranking.

iii. Assess data access and data sharing policies for essential facility implications; ensure licensing terms for proprietary datasets are not exclusionary.

iv. Review AI acquisitions for deal value threshold triggers and for data concentration/talent lock-in effects that may attract CCI scrutiny.

v. Monitor CCI market study outputs on digital markets and digital platforms for emerging enforcement priorities in AI.

CHAPTER SEVEN
TRAI's Regulatory Framework for AI in Telecommunications

7.1 Introduction: AI in Telecommunications

The telecommunications sector is both a major deployer of AI systems and a critical infrastructure upon which AI services depend. Telecom operators in India use AI for network management and optimisation, predictive maintenance, customer experience management, fraud detection, and spam filtering. The Telecom Regulatory Authority of India (TRAI) has engaged with AI governance through recommendations, consultation papers, and the implementation of AI/blockchain-based solutions for unsolicited commercial communication (UCC) filtering.[73]

TRAI — Recommendations on Regulatory Framework for AI in Telecom (2023)

Recommends that: (i) telecom operators adopt AI governance frameworks aligned with ITU-T recommendations; (ii) AI systems in telecom be subject to transparency and explainability requirements; (iii) AI-driven network management systems comply with network neutrality principles; (iv) AI-based spam and UCC detection systems achieve minimum accuracy standards; (v) customer-facing AI systems provide human escalation options. Recommends creation of a national AI governance framework for telecom as part of a broader sectoral AI policy.

7.2 AI in Network Management and Net Neutrality

TRAI's 2017 Recommendations on Network Neutrality establish that telecom service providers must not discriminate in traffic management on the basis of content, source, or application. AI-driven traffic management systems — which may prioritise, deprioritise, or throttle specific data flows — must be designed to comply with these network neutrality principles.[74]

An AI network management system that deprioritises traffic from specific OTT applications (e.g., video streaming competitors of the operator's own service) in favour of the operator's affiliated services would violate network neutrality principles. AI traffic shaping must be

[73] TRAI, "Recommendations on Regulatory Framework for Artificial Intelligence in Telecommunication Sector" (October 2023) (hereinafter "TRAI AI Recommendations 2023").

[74] TRAI, "Recommendations on Network Neutrality" (November 2017) (applicable to AI-driven traffic management).

implemented only for technical purposes — congestion management, security — and not for commercial discrimination.

7.3 The DLT Framework: AI and Spam Filtering

The Telecom Commercial Communications Customer Preference Regulations, 2018 (TCCCPR 2018) introduced a Distributed Ledger Technology (DLT) platform for the management of unsolicited commercial communications (UCC), operationalised through a combination of AI, blockchain, and consent management architecture. The DLT platform uses AI to classify SMS and voice communications, detect non-compliant senders, and enforce customer preferences.[75]

For businesses deploying AI-powered marketing communication systems, TRAI's DLT framework imposes specific compliance requirements: registration on the DLT platform, scrubbing communications against the customer preference database, and content template registration. AI systems that auto-generate personalised marketing communications must ensure that each communication variant is registered as a distinct template or falls within an approved template category.

7.4 Jurisdiction over AI-Driven OTT Services

TRAI's Recommendations on OTT Communication Services address the regulatory status of AI-powered communication platforms — including AI chatbots, virtual assistants, and automated calling systems. TRAI's recommendation is for a "light touch" regulatory framework for OTT services, but the applicability of TRAI's UCC regulations to AI-generated communications remains a point of regulatory interpretation.[76]

Bharti Airtel Ltd. v. TRAI	
Citation	(2015) 2 SCC 23
Forum	Supreme Court of India
Year	2015

[75]TRAI, "Regulation on Unsolicited Commercial Communications" (TCCCPR, 2018, as amended 2021) (DLT-based spam filtering using AI/blockchain).

[76]TRAI, "Recommendations on Regulatory Framework for Over-the-Top Communication Services" (September 2020).

Ratio Decidendi

TRAI's jurisdiction extends to the regulation of all activities of telecom service licensees, including services, charges, and practices. TRAI's power to issue regulations and directions covers technical and commercial aspects of service delivery and extends to new services delivered over licensed network infrastructure.

Regulatory Significance: Establishes the breadth of TRAI's regulatory jurisdiction, which encompasses AI systems deployed by telecom operators in service delivery. AI-powered network functions, customer service systems, and fraud detection tools operated by licensed telecom service providers are within TRAI's regulatory ambit.

7.5 Compliance Matrix: TRAI Regulation of AI in Telecommunications

The following compliance matrix sets out the key obligations, applicable legal instruments, required standards, risk classifications, and mandatory actions for entities operating in this regulatory domain:

Compliance Obligation	Legal Instrument	Standard / Threshold	Risk Level	Required Action
AI traffic management — network neutrality compliance	TRAI Net Neutrality Recommendations 2017; TRAI Act s 11	No discrimination by content, source, or application; technical management only	**Critical**	Design AI traffic management for technical purposes only; document justification for each policy; audit for commercial discrimination annually
DLT platform registration for AI marketing communications	TCCCPR 2018	All commercial communications scrubbed against DLT platform; template	**High**	Register on DLT platform; register all AI-generated message templates; implement

Compliance Obligation	Legal Instrument	Standard / Threshold	Risk Level	Required Action
		registration mandatory		automated DNC scrubbing before each communication batch
AI spam detection — TRAI accuracy standards	TCCCPR 2018, Reg. 3	Operators to implement AI spam detection meeting TRAI accuracy benchmarks	**High**	Deploy AI spam classifier calibrated to TRAI benchmarks; report performance in quarterly TRAI filings; retrain models as spam patterns evolve
Customer-facing AI — human escalation option	TRAI AI Recommendations 2023; CPA 2019	AI customer service must offer human agent escalation option	**Medium**	Build human escalation pathways into all AI customer service systems; monitor escalation fulfilment rates; include in quality of service reporting
AI governance framework — TRAI and ITU-T alignment	TRAI AI Recommendations 2023	Telecom AI governance aligned with ITU-T Focus Group on AI recommendations	**Medium**	Map governance framework to ITU-T recommendations; engage TRAI consultations proactively;

Compliance Obligation	Legal Instrument	Standard / Threshold	Risk Level	Required Action
				designate TRAI liaison for AI matters

7.6 Practitioner's Checklist: TRAI Compliance for AI in Telecom

i. Ensure AI-driven traffic management systems are designed and calibrated to comply with TRAI's network neutrality principles; document the technical justification for any traffic management.

ii. Register on the DLT platform and ensure AI-generated marketing communications comply with TCCCPR 2018 template registration and UCC scrubbing requirements.

iii. Review AI customer service systems for compliance with TRAI's quality of service standards and human escalation requirements.

iv. Monitor TRAI's evolving AI governance recommendations for telecom and ensure that AI governance frameworks are updated to reflect new standards as they are issued.

CHAPTER EIGHT
Intellectual Property Rights and Artificial Intelligence in India

8.1 Introduction: The IP Dimensions of AI

The intersection of artificial intelligence with intellectual property law raises foundational questions that have been resolved in few jurisdictions and remain largely open in India. Three distinct issues demand attention: (i) whether AI-generated works attract copyright protection, and if so, who owns that copyright; (ii) whether AI systems can be inventors for the purposes of patent law, and whether AI-generated inventions are patentable; and (iii) whether the training of AI models on copyrighted works constitutes infringement, or is protected by the fair dealing provisions of the Copyright Act.[77]

8.2 Copyright in AI-Generated Works

8.2.1 The Authorship Problem

Section 2(d) of the Copyright Act defines "author" for various categories of works. Crucially, Section 2(d)(vi) provides that for "computer-generated" literary, dramatic, musical, or artistic works, the "author" is "the person who causes the work to be created." This provision, enacted in 1994, is the primary legal hook for ownership of AI-generated works in India.[78]

The question is whether a generative AI system, operating with substantial autonomy, produces works that are "computer-generated" within Section 2(d)(vi), or whether it produces works that have no human author and therefore attract no copyright. The "modicum of creativity" standard articulated in Eastern Book Company v. D.B. Modak requires that a work involve "some degree of creativity, however small" to attract copyright protection.[79]

Eastern Book Company v. D.B. Modak	
Citation	(2008) 1 SCC 1

[77]Copyright Act, 1957, No. 14 of 1957 (India) (hereinafter "Copyright Act").

[78]Copyright Act, s 2(d)(vi) (computer-generated works: "author" deemed to be the person who causes the work to be created).

[79]Eastern Book Company v. D.B. Modak, (2008) 1 SCC 1 (India) (on the "modicum of creativity" test for copyright subsistence — applicable to AI-generated works).

Forum	Supreme Court of India
Year	2008

Ratio Decidendi

Copyright in a work does not subsist by mere labour, skill, or capital; the work must possess a "minimum degree of creativity." The test is not originality in the sense of novelty, but originality in the sense of the author's creative expression — the expression must originate from the author and not be merely mechanical reproduction. Headnotes and editorial additions that required creative legal judgment qualified; mere copy-editing of judgments did not.

Regulatory Significance: The creativity standard applies to AI-generated works in India. An AI system that produces a genuinely novel and creatively selected output may produce a work that qualifies for copyright protection under s 2(d)(vi), with the "person who causes the work to be created" — typically the AI operator or the user whose prompt triggered the output — as the deemed author. Purely mechanical or statistical outputs with no creative selection may fail the creativity threshold.

8.2.2 Ownership of AI-Generated Works

Where a work qualifies as computer-generated under Section 2(d)(vi), ownership vests in the "person who causes the work to be created." This is typically the entity operating the AI system — the AI developer or the user who provides the creative prompt — rather than the end user who receives the output as a service. Terms of service governing AI-generated content typically address this question contractually.[80]

The practical implication for AI businesses is significant: if the AI developer is the "person causing the work to be created," then the developer owns copyright in all AI-generated outputs unless contractually assigned to users. Most consumer-facing AI services contractually assign output ownership to users, but enterprise and API deployments may retain AI developer ownership.

8.3 AI Training Data and Copyright Infringement

The most commercially consequential IP question in Indian AI law is whether training AI models on copyrighted works without licence constitutes copyright infringement. The answer turns on (i) whether the training process involves "reproduction" within the meaning of Section 14 of the Copyright Act; and (ii) whether the fair dealing defence in Section 52 applies.[81]

Training a large language model or image generation model involves storing copies of training data in computer memory (reproduction), processing those copies to extract statistical features (derivative copying), and incorporating those features into model weights. The first stage — initial ingestion and storage — almost certainly constitutes "reproduction" within Section 14(b) (in respect of computer programmes) or Section 14(a)(i) (in respect of literary works).

The fair dealing defence in Section 52(1)(a) permits reproduction for purposes of "research or private study." Whether AI model training constitutes "research" is debated. The Section 52(1)(aa) exception for transient or incidental copies does not apply to the systematic copying involved in model training. Indian law does not contain a "text and data mining" exception analogous to Article 4 of the EU DSM Directive.

In the absence of judicial authority directly on point, practitioners advising AI developers should proceed on the basis that: (i) training on copyrighted works without licence carries meaningful infringement risk; (ii) the fair dealing defence provides limited protection; and (iii) the safest approach is to use licensed datasets, public domain content, or datasets whose terms of service permit AI training use.

8.4 AI and Patent Law

8.4.1 Section 3(k) and AI Patentability

Section 3(k) of the Patents Act excludes from patentability "a mathematical or business method or a computer programme per se or algorithms." The Indian Patent Office and courts have interpreted this provision as a limitation on software patents generally, though the "per se" qualifier has created space for patents on computer-implemented inventions with a "technical effect."[82]

[81]Copyright Act, s 52(1)(a) (fair dealing for research or private study); s 52(1)(aa) (transient or incidental storage) — applicability to AI training data.

[82]The Patents Act, 1970, No. 39 of 1970 (India) (hereinafter "Patents Act"), s 3(k) (exclusion of computer programmes per se from patentability).

The Delhi High Court's decision in Ferid Allani established the "technical effect" test: a computer programme that produces a technical contribution — a discernible technical advancement — may be patentable notwithstanding Section 3(k). AI systems and ML models that produce technical effects — such as novel drug molecule identification, image compression algorithms, or real-time industrial control systems — may qualify for patent protection if the technical contribution is adequately articulated in the claims.[83]

8.4.2 AI as Inventor: The DABUS Problem

The question of whether an AI system can be named as inventor in a patent application has not been resolved in Indian law. The US Court of Appeals for the Federal Circuit held in Thaler v. Vidal that US patent law requires a human inventor. The UK Supreme Court reached the same conclusion in Thaler v. Comptroller-General of Patents. In India, the Patents Act defines "inventor" as a person, which arguendo requires a human inventor. AI-generated inventions are therefore most safely claimed with the human directing the AI as the named inventor, with the AI system's role disclosed in the specification.[84]

8.5 Compliance Matrix: Intellectual Property Rights and AI

The following compliance matrix sets out the key obligations, applicable legal instruments, required standards, risk classifications, and mandatory actions for entities operating in this regulatory domain:

Compliance Obligation	Legal Instrument	Standard / Threshold	Risk Level	Required Action
Training data copyright infringement assessment	Copyright Act 1957, ss 14, 51, 52	Reproduction of copyrighted works without licence = infringement;	Critical	Audit all training datasets; obtain licences for copyrighted works; document fair

[83]Ferid Allani v. Union of India, W.P.(C) 7/2014 (Del. HC, 2019) (on the patentability of software and the "technical effect" test under s 3(k) of the Patents Act).

[84]Cf. Thaler v. Vidal, 43 F.4th 1207 (Fed. Cir. 2022) (US Court of Appeals, Federal Circuit) (AI system DABUS cannot be an "inventor" under US patent law; requires a human inventor).

Compliance Obligation	Legal Instrument	Standard / Threshold	Risk Level	Required Action
		fair dealing (s 52) provides limited protection		dealing analysis for each unlicensed source; use public domain datasets where possible
AI-generated work — copyright ownership allocation	Copyright Act 1957, s 2(d)(vi)	Author = person who causes computer-generated work to be created; creativity threshold required	**Medium**	Establish contractual IP ownership allocation in AI service agreements; register significant AI-generated works; maintain evidence of creative input to support copyright claim
Patent filing strategy for AI technical inventions	Patents Act 1970, s 3(k); Ferid Allani v. UoI (Del. HC 2019)	Technical effect must be articulated in claims; algorithms per se not patentable	**Medium**	File within 12 months of invention; frame claims around technical contribution; name human inventor; disclose AI role in specification under s 8 disclosure obligations
AI inventorship disclosure in patent applications	Patents Act 1970, s 6	Human inventor must be named; AI role	**Medium**	Establish internal AI inventorship policy; identify human inventors in AI-

Compliance Obligation	Legal Instrument	Standard / Threshold	Risk Level	Required Action
		disclosed in specification		assisted innovations; describe AI contribution in patent specification
Trade secret protection for AI models and datasets	Contract law; IT Act 2000, s 43; BNS s 316	Reasonable measures to maintain confidentiality of proprietary AI assets	**High**	Implement NDA requirements for AI system access; restrict model weight access to authorised personnel; document secrecy measures; classify AI assets as trade secrets
Trademark clearance for AI-generated brand assets	Trade Marks Act 1999, ss 9, 11	AI-generated marks subject to same distinctiveness and clearance requirements as human-created marks	**Medium**	Conduct full trademark search for AI-generated brand assets before commercial use; file trademark applications; monitor for infringement

8.6 Practitioner's Checklist: IP Compliance for AI Businesses

i. Conduct a training data audit: identify all training dataset sources, verify licensing terms, and assess copyright infringement risk from unlicensed copyrighted content.

ii. Establish contractual ownership allocation for AI-generated outputs in all AI service agreements.

iii. File patent applications for AI-driven technical inventions, framing claims around the technical effect rather than the algorithm or programme per se.

iv. Name human inventors in AI-assisted patent applications; disclose AI's role in the invention process.

v. Review AI brand asset generation tools for trademark clearance obligations before commercial use.

CHAPTER NINE

Criminal Liability, AI-Enabled Offences, and AI Evidence in Indian Courts

9.1 Introduction: Criminal Law in the Age of AI

The Bharatiya Nyaya Sanhita, 2023 (BNS), the Bharatiya Nagarik Suraksha Sanhita, 2023 (BNSS), and the Bharatiya Sakshya Adhiniyam, 2023 (BSA), which replaced the IPC, CrPC, and Indian Evidence Act respectively with effect from July 2024, have modernised but not comprehensively addressed criminal liability in AI contexts. The criminal law framework applicable to AI-enabled offences is a compound of the new criminal codes, the IT Act, the PMLA, and judge-made evidentiary standards.[85]

9.2 AI-Enabled Criminal Offences

9.2.1 Identity Fraud and Deepfakes

Section 66C of the IT Act criminalises identity theft through computer resources, and Section 66D criminalises cheating by personation using computer resources. These provisions, read with BNS Section 319 (cheating by personation), create a robust criminal framework applicable to AI-generated deepfake identity fraud — including AI voice cloning used to impersonate individuals in fraud schemes, and AI-generated synthetic identities used in KYC circumvention.[86]

Prosecution under Section 66D requires proof that the accused used a computer resource to deceive the victim into believing they were dealing with the legitimate identity. For deepfake-enabled frauds, the prosecution must prove: (i) the use of an AI system to generate the false identity; (ii) that the accused either created or deployed the AI deepfake; and (iii) that the victim was deceived. The standard of proof is beyond reasonable doubt.

[85]Bharatiya Nyaya Sanhita, 2023 (BNS) (replacing IPC 1860); Bharatiya Nagarik Suraksha Sanhita, 2023 (BNSS) (replacing CrPC 1973); Bharatiya Sakshya Adhiniyam, 2023 (BSA) (replacing Indian Evidence Act 1872).

[86]IT Act, s 66C (identity theft); s 66D (cheating by personation using computer resource) — AI deepfake identity theft.

9.2.2 AI-Generated Defamation

BNS Section 356 criminalises defamation, defined as the making or publishing of an imputation concerning a person in the knowledge or belief that it will harm the person's reputation. AI systems that generate defamatory content — including deepfake videos, fabricated news reports, or synthetic social media posts — may constitute instruments of criminal defamation.[87]

The attribution question is critical: criminal defamation requires a person to have made or published the defamatory imputation. Where an AI system autonomously generates defamatory content, the question is whether the AI developer, the platform operator, or the user who prompted the generation bears criminal liability. The prevailing analysis is that the person who "causes" the AI to generate and publish the content bears liability, subject to mens rea requirements.

9.3 AI Evidence: Admissibility and Reliability

9.3.1 Electronic Evidence Framework

The BSA, Section 63 provides for the admissibility of electronic records as evidence, replacing Section 65B of the Indian Evidence Act. Section 65A (now BSA Section 57) governs the admissibility of computer-generated documents and records. The Section 65B certificate requirement — requiring a responsible official to certify the manner in which electronic records were produced — remains foundational to the admissibility of AI-generated evidence.[88]

Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal	
Citation	(2020) 7 SCC 1
Forum	Supreme Court of India (Three-Judge Bench)
Year	2020
Ratio Decidendi *A Section 65B certificate is a mandatory condition precedent to the admissibility of electronic evidence, not merely a rule of evidence. Without the certificate, electronic records —*	

[87]BNS, s 356 (criminal defamation) — applicable to AI-generated defamatory content.

[88]BSA, s 63 (electronic records as evidence); s 65A (special provisions for electronic evidence).

irrespective of their intrinsic probative value — are inadmissible. The certificate must be given by the person responsible for the operation of the computer system producing the record. Where the certificate is not obtainable from a third party holding the data, the court may direct its production.

Regulatory Significance: AI-generated outputs tendered as evidence in civil or criminal proceedings must be accompanied by a Section 65B/BSA certificate. The certificate must be given by a responsible official of the entity operating the AI system. Parties seeking to rely on AI-generated forensic outputs, AI surveillance records, or AI-generated trading data in litigation must ensure that the certificate is obtained in the correct form before proceedings commence.

9.3.2 AI Forensic Evidence and Expert Opinion

The BSA Section 57 (formerly IEA Section 45) provides for the relevance of expert opinion. AI-generated forensic evidence — DNA match probabilities generated by AI, facial recognition match outputs, AI-based voice identification, and AI-generated document authenticity assessments — is typically presented through an expert witness who vouches for the AI system's methodology and output.[89]

Courts must be alert to the limitations of AI forensic evidence: error rates, training data biases, and the opacity of deep learning models may affect the reliability of AI forensic outputs. The persuasive analogy of the US Daubert standard — requiring that expert scientific evidence be based on a methodology that is testable, peer-reviewed, has a known error rate, and is generally accepted in the relevant scientific community — has been applied in Indian courts to assess the reliability of scientific expert evidence.

9.3.3 Deepfake Evidence and Authenticity Challenges

The proliferation of AI deepfake technology has created a new category of evidentiary challenge: the authentication of video, audio, and image evidence in civil and criminal proceedings. A party against whom deepfake evidence is tendered must be able to challenge its authenticity. Indian courts have not yet developed a settled framework for deepfake authentication, but the general

[89]BSA, s 57 (relevance of expert opinion); applicable to AI-generated forensic outputs presented through expert witnesses.

authentication requirements under the BSA — that electronic records be shown to be what they purport to be — apply.

Practitioners should anticipate that deepfake authentication challenges will become routine in high-stakes civil and criminal proceedings. AI forensic tools for deepfake detection are already available and will need to be deployed through expert witnesses in appropriate cases.

9.4 Compliance Matrix: Criminal Liability and AI Evidence

The following compliance matrix sets out the key obligations, applicable legal instruments, required standards, risk classifications, and mandatory actions for entities operating in this regulatory domain:

Compliance Obligation	Legal Instrument	Standard / Threshold	Risk Level	Required Action
Criminal liability risk assessment for AI harmful content	BNS ss 318, 319, 356; IT Act ss 66C, 66D, 66E, 67	Criminal liability where AI output constitutes cheating, personation, defamation, or obscenity	**Critical**	Conduct criminal liability audit of generative AI outputs; implement content classifiers for prohibited categories; document liability allocation in terms of service
Deepfake criminal liability prevention	IT Act ss 66C, 66E; BNS ss 319, 77	Non-consensual intimate deepfakes and AI identity theft are criminal offences	**Critical**	Implement deepfake detection at upload/generation stage; prohibit non-consensual intimate deepfakes; establish rapid takedown and

Compliance Obligation	Legal Instrument	Standard / Threshold	Risk Level	Required Action
				law enforcement cooperation protocol
AI evidence — BSA certificate procurement	BSA 2023, s 63; Arjun Panditrao (2020) 7 SCC 1	Certificate mandatory as condition precedent to admissibility of AI-generated records	**High**	Establish standing BSA certificate procedure; identify responsible official for each AI system; maintain chain of custody records for all AI-generated evidence
AI forensic evidence reliability framework	BSA 2023, s 57 (expert opinion)	AI forensic methodology must be testable, validated, with known error rate	**High**	Retain AI forensic experts with published methodology; assess opposing AI forensic evidence for validation data; prepare reliability challenge submissions for court proceedings
PMLA compliance for AI financial monitoring	PMLA 2002, ss 3, 12; RBI KYC Master Circular	AI AML systems must detect and report suspicious transactions to	**Critical**	Validate AI AML system against current PMLA typologies; conduct annual PMLA audit; maintain STR submission records;

Compliance Obligation	Legal Instrument	Standard / Threshold	Risk Level	Required Action
		FIU-IND standards		train compliance staff on AI system outputs
AI-assisted fraud prevention and liability management	BNS s 318; IT Act s 66; Contract Act 1872, s 17	AI systems used to deceive may create vicarious criminal and civil liability for operators	**High**	Review all third-party-facing AI systems for fraud risk; implement fraud detection controls; document preventive measures in compliance register; obtain specialist criminal counsel opinion

9.5 Practitioner's Checklist: Criminal Law and AI Evidence

i. Advise AI developers and operators on criminal exposure for AI-generated identity fraud, defamation, and deepfake content; assess mens rea exposure in each operational scenario.

ii. Ensure Section 65B/BSA certificates are obtained for all AI-generated evidence before litigation commences.

iii. Retain AI forensic expert witnesses for proceedings involving AI-generated evidence; assess the reliability methodology of opposing AI forensic outputs.

iv. Advise clients on deepfake detection tools and procedures for challenging the authenticity of AI-generated evidence.

CHAPTER TEN

Consumer Protection, Healthcare AI, and Liability for AI Outputs

10.1 Consumer Protection Framework for AI

10.1.1 The Consumer Protection Act, 2019 and AI Services

The Consumer Protection Act, 2019 (CPA 2019) applies to all goods and services purchased for personal use. AI-powered services — AI chatbots, robo-advisory platforms, AI diagnostic tools, AI-powered e-commerce recommendations — are "services" within the meaning of Section 2(42) of the Act, and persons using such services for personal purposes are "consumers" entitled to its protections.[90]

Section 2(17) defines "deficiency" in service as any failure, fault, imperfection, or inadequacy in quality, nature, and manner that is required to be maintained under any law or undertaken by the service provider. An AI service that provides materially inaccurate outputs, fails to perform its represented function, or produces outputs that cause harm to the consumer may constitute a "deficient service" under the Act.[91]

M/s Spring Meadows Hospital v. Harjol Ahluwalia	
Citation	(1998) 4 SCC 39
Forum	Supreme Court of India
Year	1998
Ratio Decidendi *Medical services rendered for consideration constitute a "service" under consumer protection law, and any negligence or deficiency in the rendering of such services gives rise to a consumer complaint. The court held that the standard of care applicable to medical service providers is that of a reasonably skilled professional, and that failure to meet this standard constitutes a "deficiency of service." The principle extends to all professional services.*	

[90]Consumer Protection Act, 2019, No. 35 of 2019 (India) (hereinafter "CPA 2019").

[91]CPA 2019, s 2(7) (definition of "consumer" — includes purchasers of digital services); s 2(17) (definition of "deficiency" in service).

Regulatory Significance: Foundational authority for consumer liability of AI service providers. An AI-powered medical diagnostic service, legal research AI, financial advisory AI, or any AI service representing itself as providing professional-level outputs is held to the standard of a reasonably skilled professional in the relevant domain. Outputs that fall below this standard may constitute deficient services under the CPA 2019.

10.1.2 Dark Patterns and AI Design

The CCPA's Dark Patterns Guidelines of November 2023 prohibit the use of "dark patterns" — design practices that manipulate or deceive users into taking actions they did not intend. AI systems are both potential vectors for dark patterns and potential tools for detecting them. AI-powered user interface designs that use personalised manipulation techniques — exploiting cognitive biases, creating false urgency, or obscuring cancellation options — may violate the Dark Patterns Guidelines.[92]

AI systems trained on conversion-optimisation data may independently discover and deploy dark patterns without explicit instruction. Operators of AI-driven UI systems must audit AI-generated interface adaptations for compliance with the Dark Patterns Guidelines and must not permit AI systems to implement prohibited design techniques regardless of their efficacy in increasing conversions.

10.1.3 Product Liability for AI Systems

Section 84 of the CPA 2019 imposes product liability on manufacturers and service providers for harm caused by defective products or deficient services. An AI system is a "product" (if supplied as software) and its output is a component of the "service" provided. Where an AI system causes physical, financial, or reputational harm to a user through a defect — whether in the training data, the model architecture, or the deployment configuration — the developer or operator faces product liability exposure.[93]

The doctrinal question is whether the AI system's defect was a "manufacturing defect" (incorrect at point of release), a "design defect" (systematically harmful by design), or a "warning defect" (inadequate disclosure of limitations). Each category triggers distinct liability under Section 84.

[92]Central Consumer Protection Authority (CCPA), "Guidelines for Prevention and Regulation of Dark Patterns" (November 2023) (hereinafter "Dark Patterns Guidelines").

[93]CPA 2019, s 17 (product liability — applicable to AI systems as products); s 84 (product liability action).

AI operators should implement product defect detection and recall procedures analogous to those applied in traditional products liability contexts.

10.2 Healthcare AI: Regulatory Framework

10.2.1 AI as Software as Medical Device

AI systems used for medical diagnosis, treatment recommendation, or clinical decision support are classified as "Software as Medical Device" (SaMD) under the Drugs and Cosmetics (Amendment) Rules, 2017. The Central Drugs Standard Control Organisation (CDSCO) has issued draft guidance on AI/ML-based SaMD, drawing on the US FDA's proposed regulatory framework for AI/ML-based SaMD and the EU's MDR framework.[94]

CDSCO — Guidance Document for AI/ML-Based Software as Medical Device (Draft) (2023)

Classifies AI/ML-based SaMD by risk level. High-risk SaMD (Class C) — systems providing diagnosis or treatment recommendations for life-threatening conditions — require pre-market approval, clinical validation studies, and ongoing post-market surveillance. Requires algorithmic transparency, explainability of diagnostic outputs to clinicians, bias assessment across demographic subgroups, and labelling of AI-generated clinical recommendations. Mandates continuous learning systems to have "predetermined change control plans" approved by CDSCO before model updates are deployed.

10.2.2 Telemedicine and AI-Assisted Clinical Practice

The Telemedicine Practice Guidelines, 2020 (issued under the NMC Act and the IMC Act) govern AI-assisted telemedicine. AI tools used in teleconsultation — symptom checkers, diagnostic aids, prescription recommendation systems — must comply with the Guidelines and are subject to the Medical Council of India's standards of professional practice. A registered medical practitioner who relies on an AI diagnostic tool remains professionally responsible for the clinical decision; AI provides decision support, not a substitute for clinical judgment.[95]

[94]Central Drugs Standard Control Organisation (CDSCO), "Guidance Document for AI/ML-Based Software as Medical Device" (2023 Draft) (hereinafter "CDSCO AI Guidance").

[95]National Medical Commission Act, 2019 (NMC Act); Telemedicine Practice Guidelines, 2020 (applicable to AI-assisted telemedicine).

10.3 Compliance Matrix: Consumer Protection and Healthcare AI

The following compliance matrix sets out the key obligations, applicable legal instruments, required standards, risk classifications, and mandatory actions for entities operating in this regulatory domain:

Compliance Obligation	Legal Instrument	Standard / Threshold	Risk Level	Required Action
Consumer service quality — AI deficiency prevention	CPA 2019, ss 2(17), 42; Spring Meadows Hospital (1998) 4 SCC 39	AI service must meet standard of reasonably skilled professional in relevant domain	**High**	Establish AI quality benchmarks; conduct periodic accuracy and performance audits; implement user feedback and complaint tracking system
Dark patterns prohibition in AI-driven interfaces	CPA 2019, s 2(47); CCPA Dark Patterns Guidelines (2023)	Prohibition on false urgency, hidden subscription, confirm-shaming, and other manipulative AI design patterns	**High**	Audit AI-generated UI adaptations against Dark Patterns Guidelines; disable AI optimisation for prohibited patterns; implement quarterly compliance review
Product liability — AI system defect management	CPA 2019, s 84	Developer/operator liability for manufacturing defect, design defect, or warning	**High**	Implement pre-deployment defect testing; maintain model defect registry; establish

Compliance Obligation	Legal Instrument	Standard / Threshold	Risk Level	Required Action
		defect in AI system		AI product recall procedure; obtain product liability insurance cover
Healthcare AI — SaMD classification and CDSCO approval	Drugs and Cosmetics Act 1940; CDSCO AI/ML SaMD Guidance (Draft 2023)	Class C (high-risk): pre-market approval; clinical validation; post-market surveillance mandatory	**Critical**	Classify AI healthcare product by risk per CDSCO guidance; file pre-market application for Class B/C products; establish post-market surveillance programme
Telemedicine AI — physician oversight and NMC compliance	Telemedicine Practice Guidelines 2020; NMC Act 2019	AI provides decision support only; registered physician retains clinical responsibility	**Critical**	Design AI clinical tools as physician decision-support only; disclose AI nature to clinicians; ensure physician sign-off on AI clinical recommendations; maintain audit trail
AI advertising — misleading claims prevention	CPA 2019, s 2(28); CCPA Misleading Advertising	AI-generated advertising must not contain false, misleading, or	**High**	Implement pre-publication review of AI-generated advertising; fact-check AI claims

Compliance Obligation	Legal Instrument	Standard / Threshold	Risk Level	Required Action
	Guidelines (2022)	unsubstantiated claims		before publication; establish advertiser liability framework in platform T&Cs
AI value chain — contractual liability allocation	CPA 2019, s 84; Contract Act 1872; IT Act s 79	Clear contractual allocation of AI liability across developer, operator, and user	**High**	Include AI-specific liability allocation, indemnity, and warranty provisions in all supply chain agreements; obtain representations on model validation and regulatory compliance

10.4 Liability Allocation in the AI Value Chain

The AI value chain involves multiple parties: foundation model developers, fine-tuning entities, platform operators, application developers, and end users. Liability for harm caused by AI outputs must be allocated across this chain, and the allocation will depend on the nature of the defect, the contractual arrangements between parties, and the applicable regulatory framework.

Practitioners advising AI businesses should ensure that commercial agreements governing AI supply chains include: (i) clear allocation of responsibility for model performance and output accuracy; (ii) indemnification provisions covering third-party claims arising from AI outputs; (iii) representations and warranties as to model validation, bias testing, and regulatory compliance; and (iv) incident response and remediation obligations.

CHAPTER ELEVEN

Consolidated Regulatory Matrix and Practitioner's Framework

11.1 Introduction

The preceding chapters have surveyed the full landscape of India's regulatory framework for AI businesses across ten distinct domains. This concluding chapter consolidates the analysis into a unified regulatory matrix, identifies the cross-cutting principles that govern AI regulation in India, and proposes a practitioner's framework for AI compliance management.[96]

11.2 Consolidated Regulatory Matrix

The following matrix maps the principal regulators, applicable instruments, regulatory scope, and enforcement powers across India's AI regulatory landscape:

Regulator	Key Instruments	AI Scope	Enforcement Powers
MeitY / DPDPB	DPDPA 2023; IT Act 2000; IT Rules 2021	Data processing; Intermediary liability; Cybersecurity; Deepfakes; AI content	Up to INR 250 crore (DPDPA); Takedown orders; Criminal prosecution (IT Act)
SEBI	SEBI Act 1992; AI/ML Circular 2019; Algo Trading Framework	AI in capital markets; Robo-advisory; HFT; Market surveillance	Monetary penalties; Suspension; Deregistration; SAT appeal
RBI	RBI Act; Banking Regulation Act; Digital Lending Circular 2022; IT	AI in banking, credit, KYC, AML, payments	Monetary penalties; Business restrictions; RBI Act s 35A directions

[96]Niti Aayog, "Responsible AI for All: Implementing the Principles" (2021) Annex — Regulatory Matrix.

Regulator	Key Instruments	AI Scope	Enforcement Powers
	Governance Draft 2023		
CCI	Competition Act 2002 (as amended 2023)	Algorithmic collusion; AI dominance abuse; Data access refusal; AI M&A	Penalty up to 10% of average 3-yr turnover; Structural remedies; Behavioural orders
TRAI	TRAI Act 1997; TCCCPR 2018; Net Neutrality Recommendations	AI in telecom networks; Spam filtering; OTT regulation	Directions; Financial penalties under TRAI Act; Licence revocations
IRDAI	Insurance Act 1938; IRDAI Regulations	AI in underwriting; Claims assessment; Fraud detection in insurance	Regulatory actions under Insurance Act; Penalty; Licence suspension
PFRDA	PFRDA Act 2013; NPS Regulations	AI in pension fund management; Robo-advisory for NPS subscribers	Directions; Penalty; Disqualification of intermediaries
CDSCO / MOH	Drugs & Cosmetics Act 1940; SaMD Guidance 2023	AI diagnostic software; Clinical AI; Healthcare AI apps	Pre-market approval denial; Recall; Criminal prosecution
CCPA	Consumer Protection Act 2019; Dark Patterns Guidelines 2023	Consumer-facing AI services; AI dark patterns; AI advertising	Cease and desist; Penalty; Recall of AI product/service
NMC / IMC	NMC Act 2019; Telemedicine Guidelines 2020	AI-assisted telemedicine; Clinical AI tools used by doctors	Professional misconduct; Deregistration of medical practitioners

11.3 Cross-Cutting Principles of Indian AI Regulation

11.3.1 Proportionality

The constitutional proportionality standard — derived from Puttaswamy and Anuradha Bhasin — requires that any regulatory obligation imposed on an AI system be proportionate to the legitimate aim pursued. AI businesses challenging disproportionate regulatory demands have a constitutional basis for doing so, and the proportionality analysis is the practitioner's most powerful tool in regulatory engagement.

11.3.2 Explainability and Transparency

Across all regulatory domains — SEBI, RBI, DPDPA, MeitY, CDSCO — the requirement that AI system outputs be explainable and that AI decision criteria be transparent is a consistent and cross-cutting principle. Black-box AI systems face regulatory resistance across all sectors. AI businesses should treat explainability as a design requirement, not an afterthought.

11.3.3 Board-Level Accountability

From SEBI's AI/ML Circular to RBI's IT Governance Draft to the MeitY Advisory, Indian regulators consistently require board-level accountability for AI deployment. AI governance must be embedded in the highest levels of corporate governance, with the board receiving periodic reports on AI performance, risk, and compliance.

11.3.4 Non-Discrimination and Fairness

The constitutional equality guarantee under Article 14 and the anti-discrimination principles in data protection, consumer protection, and financial regulation impose a common requirement: AI systems must not produce discriminatory outcomes on the basis of protected characteristics. Bias testing and fairness auditing are compliance requirements, not optional quality measures.

11.3.5 Human Oversight

The SEBI AI/ML Circular's requirements for kill switches and human oversight of algorithmic trading, the RBI's requirements for human review of AI credit decisions, CDSCO's requirements for physician oversight of AI diagnostic tools, and the CCPA's dark pattern standards all reflect a common principle: consequential AI decisions must be subject to meaningful human oversight. AI autonomy is not an absolute value; it must be calibrated against the risk of harm.

11.4 Recommendations for AI Governance Frameworks

11.4.1 AI Governance Committee

a. Constitute a board-level AI Governance Committee with responsibility for approving AI strategy, reviewing AI risk, and ensuring regulatory compliance across all domains.

b. Appoint a Chief AI Officer or equivalent senior executive with cross-functional AI governance responsibility.

11.4.2 AI Risk Register

a. Maintain a comprehensive AI risk register cataloguing all AI systems in production, their regulatory classification, applicable obligations, validation status, and performance metrics.

b. Conduct annual AI risk assessments, including regulatory compliance reviews, bias audits, and cybersecurity assessments.

11.4.3 Regulatory Engagement

a. Proactively engage with regulators — SEBI, RBI, MeitY, CCI, TRAI — on emerging AI governance frameworks before obligations crystallise.

b. Participate in regulatory sandbox programmes where applicable to test AI products in compliant environments.

c. Monitor and respond to consultation papers issued by all relevant regulators on AI governance.

11.5 Concluding Observations

India stands at a pivotal juncture in AI governance. The country has the technical talent, the regulatory infrastructure, and the legislative ambition to become a global leader in responsible AI development. What is required is a coherent, comprehensive, and forward-looking regulatory framework that enables innovation while protecting the rights and interests of citizens, consumers, and market participants.[97]

[97]OECD AI Policy Observatory, "National AI Policies and Strategies" (2024) (India Country Note).

The multi-regulator architecture that characterises Indian financial and technology regulation is both a strength — enabling deep sectoral expertise — and a challenge, creating the risk of regulatory fragmentation, inconsistency, and gaps. The practitioner's most important contribution is to navigate this complexity with rigour, creativity, and a commitment to the rule of law.

This compendium has sought to provide the foundation for that endeavour. The law in this field will continue to evolve rapidly; practitioners are encouraged to return to first principles — constitutional, statutory, and common law — when navigating novel situations for which the existing framework provides incomplete guidance. The fundamental values of fairness, transparency, accountability, and proportionality are durable guides in a landscape of perpetual change.

— End of Compendium —

DISCLAIMER

This compendium has been prepared by EquiCorp Associates LLP for general informational purposes only. It does not constitute legal advice and is not a substitute for advice from qualified legal counsel in relation to any specific transaction, regulatory filing, or compliance question. The regulatory landscape for Artificial Intelligence (AI) businesses in India is subject to frequent and material change; readers are advised to verify the current status of all instruments cited herein before acting on any information contained in this compendium. EquiCorp Associates LLP makes no representation as to the completeness or accuracy of this compendium and disclaims any liability for reliance on its contents.