



INTERNATIONAL LAW
JOURNAL

**WHITE BLACK
LEGAL LAW
JOURNAL
ISSN: 2581-
8503**

Peer - Reviewed & Refereed Journal

The Law Journal strives to provide a platform for discussion of International as well as National Developments in the Field of Law.

WWW.WHITEBLACKLEGAL.CO.IN

DISCLAIMER

No part of this publication may be reproduced, stored, transmitted, translated, or distributed in any form or by any means—whether electronic, mechanical, photocopying, recording, scanning, or otherwise—without the prior written permission of the Editor-in-Chief of *White Black Legal – The Law Journal*.

All copyrights in the articles published in this journal vest with *White Black Legal – The Law Journal*, unless otherwise expressly stated. Authors are solely responsible for the originality, authenticity, accuracy, and legality of the content submitted and published.

The views, opinions, interpretations, and conclusions expressed in the articles are exclusively those of the respective authors. They do not represent or reflect the views of the Editorial Board, Editors, Reviewers, Advisors, Publisher, or Management of *White Black Legal*.

While reasonable efforts are made to ensure academic quality and accuracy through editorial and peer-review processes, *White Black Legal* makes no representations or warranties, express or implied, regarding the completeness, accuracy, reliability, or suitability of the content published. The journal shall not be liable for any errors, omissions, inaccuracies, or consequences arising from the use, interpretation, or reliance upon the information contained in this publication.

The content published in this journal is intended solely for academic and informational purposes and shall not be construed as legal advice, professional advice, or legal opinion. *White Black Legal* expressly disclaims all liability for any loss, damage, claim, or legal consequence arising directly or indirectly from the use of any material published herein.

ABOUT WHITE BLACK LEGAL

White Black Legal – The Law Journal is an open-access, peer-reviewed, and refereed legal journal established to provide a scholarly platform for the examination and discussion of contemporary legal issues. The journal is dedicated to encouraging rigorous legal research, critical analysis, and informed academic discourse across diverse fields of law.

The journal invites contributions from law students, researchers, academicians, legal practitioners, and policy scholars. By facilitating engagement between emerging scholars and experienced legal professionals, *White Black Legal* seeks to bridge theoretical legal research with practical, institutional, and societal perspectives.

In a rapidly evolving social, economic, and technological environment, the journal endeavours to examine the changing role of law and its impact on governance, justice systems, and society. *White Black Legal* remains committed to academic integrity, ethical research practices, and the dissemination of accessible legal scholarship to a global readership.

AIM & SCOPE

The aim of *White Black Legal – The Law Journal* is to promote excellence in legal research and to provide a credible academic forum for the analysis, discussion, and advancement of contemporary legal issues. The journal encourages original, analytical, and well-researched contributions that add substantive value to legal scholarship.

The journal publishes scholarly works examining doctrinal, theoretical, empirical, and interdisciplinary perspectives of law. Submissions are welcomed from academicians, legal professionals, researchers, scholars, and students who demonstrate intellectual rigour, analytical clarity, and relevance to current legal and policy developments.

The scope of the journal includes, but is not limited to:

- Constitutional and Administrative Law
- Criminal Law and Criminal Justice
- Corporate, Commercial, and Business Laws
- Intellectual Property and Technology Law
- International Law and Human Rights
- Environmental and Sustainable Development Law
- Cyber Law, Artificial Intelligence, and Emerging Technologies
- Family Law, Labour Law, and Social Justice Studies

The journal accepts original research articles, case comments, legislative and policy analyses, book reviews, and interdisciplinary studies addressing legal issues at national and international levels. All submissions are subject to a rigorous double-blind peer-review process to ensure academic quality, originality, and relevance.

Through its publications, *White Black Legal – The Law Journal* seeks to foster critical legal thinking and contribute to the development of law as an instrument of justice, governance, and social progress, while expressly disclaiming responsibility for the application or misuse of published content.

LEGAL CHALLENGES OF ARTIFICIAL INTELLIGENCE IN COMMERCIAL CONTRACTS

AUTHORED BY - KRISHNA PRASANTH V.N & DR.J.KIRUBA SHARMILA

Vels Institute Of Science, Technology And Advance Studies

CHAPTER I INTRODUCTION

1.1 Abstract

Artificial Intelligence (AI) is transforming commercial transactions at an unprecedented pace. Across India, AI-driven systems autonomously negotiate, draft, execute, and manage contracts in sectors ranging from financial services and insurance to e-commerce and healthcare. Yet the legal architecture governing these phenomena remains rooted in the Indian Contract Act, 1872¹ — a statute conceived in an era when contracting parties were invariably human beings capable of intention, volition, and consent. This dissertation undertakes a critical doctrinal analysis of the legal challenges that AI-generated contracts pose under Indian law, with particular emphasis on the foundational requirements of offer, acceptance, consideration, competency, and free consent, as well as the upstream questions of legal personality, liability attribution, and evidence.

The research gap motivating this study is significant: while an expanding body of scholarship addresses AI ethics and algorithmic fairness, the specific question of whether AI-generated contracts are enforceable under Indian Contract Law has received comparatively little systematic academic attention. This dissertation argues that existing statutory and common law doctrine, stretched to accommodate AI-generated contracts, produces a series of structural inadequacies — from the inability to attribute legal capacity to a software system, to the opacity of machine-learning processes that vitiates meaningful consent. Drawing on comparative analysis of the European Union, United Kingdom, United States, Singapore, and China, the dissertation formulates a six-pillar reform agenda designed to provide India with a principled, future-proof framework for AI-generated commercial contracts.

The dissertation is doctrinal in methodology, engaging primary sources — statutes, judicial decisions, and governmental reports — supplemented by comparative and normative

¹Indian Contract Act, 1872 (Act 9 of 1872), Preamble. The Act codifies the general principles of the law of contract in India and remains the primary legislation governing contractual relationships.

reasoning. It concludes with specific legislative and regulatory proposals calibrated to India's constitutional structure, economic priorities, and digital policy trajectory.

1.2 Background and Context

India stands at an inflection point in its relationship with artificial intelligence. According to NITI Aayog's National Strategy for Artificial Intelligence, the domestic AI market was valued at approximately USD 6 billion in 2023 and is projected to reach USD 28 billion by 2028.² The India AI Mission, announced in the Union Budget 2024–25, allocates INR 10,372 crores over five years for compute infrastructure, research centres, and foundational model development, signalling an unmistakable state commitment to AI-led economic growth.³ Simultaneously, private sector adoption has accelerated dramatically: the NASSCOM–Deloitte AI Adoption Index 2023 reports that 59 per cent of Indian enterprises have deployed AI in at least one core business function, up from 31 per cent in 2020.⁴

Within this landscape, AI's role in commercial contracting has moved well beyond research and experimentation. Automated trading algorithms on India's recognised stock exchanges execute millions of transactions each second without human intervention, each constituting a legally binding sale or purchase of securities.⁵ In the insurance sector, IRDAI-regulated underwriting models process and accept proposals for life and health cover with minimal human oversight.⁶ Large e-commerce platforms deploy recommendation engines and dynamic pricing algorithms that generate offers to consumers and respond to their acceptances in real time. Ride-hailing and logistics platforms use AI to match supply and demand, set fares, and generate service agreements at scale. Legal technology firms have introduced AI contract drafting and review tools that produce first drafts of commercial agreements indistinguishable from lawyer-authored documents.

²NITI Aayog, 'National Strategy for Artificial Intelligence' (Government of India, 2018) 5–7. The document projected India's AI market at USD 6 billion in 2023, growing to USD 28 billion by 2028.

³Ministry of Electronics and Information Technology, 'India AI Mission' (Government of India, 2024) 3. The Mission allocates INR 10,372 crores over five years for AI infrastructure and research.

⁴NASSCOM–Deloitte, 'AI Adoption Index India 2023' (NASSCOM 2023) 8–12.

⁵Securities and Exchange Board of India, 'Circular on Algorithmic Trading' SEBI/HO/MRD/DP/CIR/P/2018/161 (2018). ⁶Insurance Regulatory and Development Authority, 'Guidelines on Use of AI and ML in Insurance Underwriting' IRDAI/LIFE/CIR/MISC/101/2023 (2023).

The legal implications of this transformation are profound. The Indian Contract Act, 1872, despite its enduring elegance as a codification of common-law contract principles, was drafted at a time when the very concept of automated contracting was inconceivable. The Act's definitional architecture — premised on 'persons' making proposals, 'persons' accepting them, and 'parties' demonstrating capacity and free consent — offers no accommodation for systems that lack legal personality, subjective intention, or cognitive volition.⁷ The Information Technology Act, 2000, which inserted section 10A to validate electronic contracts⁸, provides only a partial solution: it establishes that contracts concluded through electronic means are not invalid merely by reason of their electronic form, but it does not address the deeper doctrinal questions of capacity, consent, and agency that arise when the contracting entity is an autonomous machine-learning system rather than a human user of an electronic medium.

Meanwhile, the global regulatory environment is evolving rapidly. The European Union's AI Act 2024 — the world's first comprehensive AI regulatory framework — introduces mandatory requirements for high-risk AI systems operating in areas including employment, essential services, and critical infrastructure.⁹ The United States has enacted the UETA, which explicitly recognises contracts formed by electronic agents.¹⁰ Singapore has revised its Electronic Transactions Act to accommodate algorithmic contracting.¹¹ India risks regulatory arbitrage and legal uncertainty if it fails to develop an equivalent framework. The present dissertation seeks to contribute to that development by systematically mapping the doctrinal gaps and proposing targeted reforms.

1.3 Statement of the Problem

The core problem is one of doctrinal misalignment. Indian Contract Law, as codified in the Act of 1872 and interpreted by over a century of judicial precedent, is structured around human contracting parties. Its foundational categories — offer, acceptance, consideration,

⁷Pollock and Mulla, *The Indian Contract and Specific Relief Acts* (15th edn, LexisNexis 2021) Vol 1, 1–8.

⁸Information Technology Act, 2000 (Act 21 of 2000), s 10A (inserted by the Information Technology (Amendment) Act 2008).

⁹European Parliament, Regulation (EU) 2024/1689 of 13 June 2024 laying down harmonised rules on artificial intelligence (AI Act) [2024] OJ L 2024/1689 (EU AI Act).

¹⁰Uniform Electronic Transactions Act (UETA) (US 1999), s 14. The provision explicitly validates contracts formed by electronic agents.

¹¹Singapore Electronic Transactions Act (ETA) (Cap 88, 2011 Rev Edn), s 11A (inserted by Electronic Transactions (Amendment) Act 2021).

competency, free consent — presuppose entities capable of subjective intent, legal personality, and volitional action. AI systems possess none of these attributes in any legally recognised sense. Consequently, when an AI system generates, negotiates, or executes a contract, it is unclear (a) whether the essential elements of a valid contract under section 10 of the Indian Contract Act are satisfied¹²; (b) which human or corporate principal is bound by the AI's actions; (c) whether the opacity of machine-learning processes undermines the free consent requirement; (d) what liability rules govern harm caused by AI contracting errors; and (e) whether the existing evidentiary framework adequately handles AI-generated documentary evidence.

These are not merely theoretical puzzles. As algorithmic contracts proliferate, courts and tribunals across India will increasingly be asked to adjudicate disputes arising from their formation and performance. In the absence of legislative guidance or settled precedent, judges must resort to analogical reasoning from doctrines developed in wholly different technological contexts, generating inconsistency and unpredictability. The problem is compounded by the multi-party nature of many AI deployments: a developer creates the AI system, a deployer integrates it into a commercial platform, and a user interacts with the platform — yet none of these actors may have specifically authorised the precise contractual terms that the AI generates in a given transaction. The doctrines of agency and privity, as understood in Indian law, are ill-equipped to resolve this tripartite responsibility gap.

1.4 Significance of the Study

This dissertation makes four principal contributions to legal scholarship and policy. First, it provides the first systematic doctrinal mapping of the enforceability challenges that AI-generated contracts pose under Indian Contract Law, filling a gap in both Indian legal scholarship and comparative AI law literature. Second, it situates the Indian problem within the global regulatory context, enabling policymakers to learn from international experience while remaining sensitive to India's distinctive constitutional structure and economic circumstances. Third, it proposes concrete, technically informed legislative amendments and regulatory guidelines that can be adopted within India's existing parliamentary and

¹²Indian Contract Act, 1872, s 10.

administrative framework. Fourth, it contributes to the theoretical debate about AI legal personhood by examining, critically and without premature conclusions, whether the attribution of a limited form of legal capacity to AI systems is necessary or desirable in the Indian context.

The practical significance of this study is no less important. As India's digital economy expands and as AI-enabled contracting becomes ubiquitous, businesses, consumers, and legal practitioners require clarity about the enforceability of AI-generated agreements, the identity of the liable party when such agreements go wrong, and the procedural rules for litigating AI-related disputes. This dissertation aims to provide that clarity by translating doctrinal analysis into actionable guidance.

1.5 Research Objectives

This dissertation pursues six specific research objectives. First, to examine whether AI-generated contracts satisfy the essential conditions of a valid contract under section 10 of the Indian Contract Act, 1872, with particular attention to offer, acceptance, consideration, competency, and free consent. Second, to analyse the doctrinal adequacy of the law of agency — as understood in India — as a mechanism for attributing legal responsibility for AI-generated contracts to human principals. Third, to evaluate the evidentiary challenges of AI-generated contracts under the Bharatiya Sakshya Adhiniyam, 2023. Fourth, to compare India's regulatory position with the approaches adopted in the European Union, United Kingdom, United States, Singapore, and China, and to identify lessons for Indian law reform. Fifth, to examine existing and proposed dispute resolution mechanisms for AI contract disputes, including litigation, arbitration, online dispute resolution, and sectoral regulatory adjudication. Sixth, to formulate a principled, constitutionally coherent reform agenda for Indian law, encompassing legislative amendments, regulatory guidelines, and judicial interpretive principles.

1.6 Research Questions

The primary research question is: Are AI-generated contracts enforceable under the Indian Contract Act, 1872, and if not, what legal reforms are necessary to provide a workable framework for such contracts?

This primary question is disaggregated into six secondary research questions:

- (i) Do AI-generated contracts satisfy the requirements of offer, acceptance, and consideration under the Indian Contract Act, 1872?
- (ii) Can an AI system be regarded as an agent for the purposes of Indian contract and agency law, and if so, what are the limits of such analogy?
- (iii) Does the opacity of machine-learning processes constitute a vitiating factor under sections 13–22 of the Indian Contract Act (free consent provisions)?
- (iv) How does Indian evidentiary law, including the Bharatiya Sakshya Adhiniyam 2023, apply to contracts generated and executed by AI systems?
- (v) What lessons can India draw from the regulatory approaches adopted in the EU, UK, US, Singapore, and China regarding AI-generated contracts?
- (vi) What specific legislative, regulatory, and judicial reforms are necessary to ensure that AI-generated contracts are enforceable, fair, and subject to effective dispute resolution in India?

1.7 Literature Review

This section reviews the relevant scholarly and policy literature under five thematic categories: (A) foundational AI and law scholarship; (B) Indian legal scholarship on AI and digital contracts; (C) ethics, governance, and policy frameworks; (D) electronic contracts and information technology law; and (E) comparative and international AI law.

A. *Foundational AI and Law Scholarship*

Chopra and White's *A Legal Theory for Autonomous Artificial Agents* (2011)¹³ remains the seminal text in the field. The authors argue that existing legal doctrine — agency, contract,

¹³Samir Chopra and Laurence White, *A Legal Theory for Autonomous Artificial Agents* (University of Michigan Press 2011) 1–15. The authors argue that current legal doctrine is ill-equipped to handle transactions initiated and completed by autonomous software agents.

tort — is inadequate to handle the actions of autonomous software agents and that a new conceptual framework is required. Their analysis of the 'will' problem — the impossibility of attributing genuine intent to a computational process — anticipates the doctrinal difficulties that this dissertation examines under Indian law. Hallevy's *When Robots Kill* (2013)¹⁴ approaches the problem from a criminal law perspective but offers insights relevant to civil liability for AI-generated harm. Abbott's *The Reasonable Robot* (2020)¹⁵ proposes the doctrine of AI neutrality, arguing that the law should treat AI and human actions equivalently to preserve incentive structures for efficient technological adoption. This dissertation engages critically with Abbott's proposal, arguing that it is premature in the Indian context where the legal infrastructure for AI accountability is underdeveloped.

The theoretical debate about AI legal personhood — whether AI systems should be accorded a form of legal capacity analogous to corporate personality — has generated a substantial literature. Solum's *Legal Personhood for Artificial Intelligences* (1992) raised the question decades before it became practically urgent. More recently, Delvaux's *European Parliament Report* (2017) recommended the creation of 'electronic personhood' for autonomous AI systems, a proposal ultimately rejected in the EU AI Act. This dissertation examines whether the concept has any utility in the Indian context and concludes that, while legislative recognition of AI as a limited legal agent for contracting purposes may be necessary, full legal personhood is neither warranted nor constitutionally straightforward.

B. Indian Legal Scholarship on AI and Digital Contracts

Indian scholarship on the intersection of AI and contract law remains nascent but is growing. Duggal's *Cyberlaw: The Indian Perspective* (2020)¹⁶ provides a comprehensive analysis of the Information Technology Act, 2000, including section 10A on electronic contracts, but predates significant AI developments and does not specifically address machine-learning-generated contracts. Kamath's *Law Relating to Computers, Internet and*

¹⁴Gabriel Hallevy, *When Robots Kill: Artificial Intelligence under Criminal Law* (Northeastern University Press 2013) 47. Hallevy examines whether AI systems can be considered perpetrators under criminal statutes.

¹⁵Ryan Abbott, *The Reasonable Robot: Artificial Intelligence and the Law* (Cambridge University Press 2020) 32–58.

¹⁶Pavan Duggal, *Cyberlaw: The Indian Perspective* (Saakshar Law Publications 2020) 112–140. Duggal analyses the enforceability of electronic contracts under the Information Technology Act, 2000.

E-Commerce (6th edition, 2022)¹⁷ updates the analysis to encompass cloud computing and platform economy issues, offering useful doctrinal groundwork. Seth's *Technology Contracts: Drafting and Negotiating in the Digital Age* (2021)¹⁸ provides a practitioner's perspective on AI contract clauses, highlighting the emerging commercial practice gap with legal doctrine.

Ambast's journal article, 'Contractual Liability in the Age of Artificial Intelligence: Indian Perspectives' (2023)¹⁹ is among the most directly relevant recent contributions. Ambast identifies the consent and competency problems as central challenges and tentatively suggests that the law of agency provides the most workable — if imperfect — solution. Mohnot's 'Electronic Contracts and Digital Commerce: Indian Legal Landscape' (2022)²⁰ examines the enforceability of click-wrap and browse-wrap agreements, which frequently incorporate AI-driven terms, and finds significant doctrinal uncertainty. Mahaseth's 'Regulating AI in India: Learning from Global Experiences' (2023)²¹ surveys international approaches and argues for a risk-based regulatory model adapted to India's administrative capacity.

Kumar's 'Smart Contracts and the Indian Legal Framework' (2022)²² examines blockchain-based smart contracts — a related but distinct category — and analyses their interaction with the Indian Contract Act, the IT Act, and the Specific Relief Act. Dalmia's 'Data as Consideration in AI Contracts: An Indian Perspective' (2023)²³ proposes that personal data exchanged in AI-driven transactions can constitute good consideration under section 2(d) of the Indian Contract Act, a conceptually innovative but doctrinally contested argument. Lath's 'Algorithmic Decision-Making and Consumer Rights in India' (2023)²⁴ examines the interaction between AI-generated commercial terms and consumer protection law, finding significant protection gaps. S Kumar's 'Artificial Intelligence and the Law of Agency in India'

¹⁷Nandan Kamath, *Law Relating to Computers, Internet and E-Commerce* (Universal Law Publishing 6th edn 2022) 89–95.

¹⁸Ranjit Seth, *Technology Contracts: Drafting and Negotiating in the Digital Age* (Wolters Kluwer India 2021) 77–89. ¹⁹Sanhita Ambast, 'Contractual Liability in the Age of Artificial Intelligence: Indian Perspectives' (2023) 15 *Indian Journal of Law and Technology* 34, 38.

²⁰Deepa Mohnot, 'Electronic Contracts and Digital Commerce: Indian Legal Landscape' (2022) 8 *National Law School of India Review* 111, 115.

²¹Harsh Mahaseth, 'Regulating AI in India: Learning from Global Experiences' (2023) 12 *Asian Journal of International Law* 201, 207.

²²Prashant Kumar, 'Smart Contracts and the Indian Legal Framework' (2022) 5 *Indian Law Review* 89, 95.

²³Vijay Pal Dalmia, 'Data as Consideration in AI Contracts: An Indian Perspective' (2023) 10 *Computer Law and Security Review* 1, 6.

²⁴Aparajita Lath, 'Algorithmic Decision-Making and Consumer Rights in India' (2023) 7 *Jindal Global Law Review* 215, 221.

(2022)²⁵ provides the most detailed examination of the agency analogy, concluding that existing doctrine can accommodate rule-based AI systems but breaks down for machine-learning systems whose behaviour is not fully predictable by the principal.

C. Ethics, Governance, and Policy Frameworks

NITI Aayog's National Strategy for Artificial Intelligence (2018)²⁶ and its subsequent Responsible AI for All reports²⁷ establish India's policy framework for AI governance, emphasising inclusion, safety, and economic growth. The documents are primarily programmatic rather than legally prescriptive, but they provide the policy context within which legislative reform must occur. The Srikrishna Committee Report (2018)²⁸ on data protection has shaped the enactment of the Digital Personal Data Protection Act, 2023²⁹, which regulates the processing of personal data — including data processed by AI systems — and has direct implications for AI-generated contracts involving personal data.

At the international level, the OECD Recommendation on AI (2019)³⁰ articulates five value-based principles for trustworthy AI, including transparency, accountability, and robustness. The UNESCO Recommendation on the Ethics of AI (2021)³¹ extends this framework to encompass human rights, environmental sustainability, and cultural diversity. The G20 New Delhi Leaders' Declaration (2023)³² includes provisions on responsible AI governance that acknowledge the need for interoperable national frameworks. The World Economic Forum's AI Governance Report (2019)³³ proposes a holistic approach that integrates

²⁵Sudhanshu Kumar, 'Artificial Intelligence and the Law of Agency in India' (2022) 4 Indian Law Journal 55, 62.

²⁶

²⁷NITI Aayog, 'Responsible AI for All: Adopting the Framework — A Use Case Approach for Responsible AI in Healthcare' (Government of India, 2022) 8–12.

²⁸Justice BN Srikrishna (Chair), 'A Free and Fair Digital Economy: Protecting Privacy, Empowering Indians' (Ministry of Electronics and Information Technology 2018) 10–15 (Srikrishna Committee Report).

²⁹Digital Personal Data Protection Act, 2023 (Act 22 of 2023), s 4.

³⁰OECD, 'Recommendation of the Council on Artificial Intelligence' OECD/LEGAL/0449 (22 May 2019). The Recommendation sets out five value-based principles for trustworthy AI.

³¹UNESCO, 'Recommendation on the Ethics of Artificial Intelligence' (UNESCO 2021) 6–8.

³²G20 New Delhi Leaders' Declaration (9–10 September 2023) para 35. The Declaration affirmed shared principles for responsible AI governance.

³³World Economic Forum, 'AI Governance: A Holistic Approach to Implement Ethics into AI' (WEF 2019) 10.

ethics into AI design, procurement, and deployment — an approach that the present dissertation argues should inform India's legislative reform agenda.

D. *Electronic Contracts and Information Technology Law*

The literature on electronic contracts provides essential doctrinal foundations for the analysis of AI-generated contracts, since AI contracts are a subset of the broader category of electronically formed agreements. Viswanathan's *Law and Commerce of Contracts* (2019) examines the interaction between the Indian Contract Act and the IT Act, particularly section 10A, and analyses the enforceability of contracts formed through automated systems. Basu and Sen's *Legal Aspects of E-Commerce in India* (2019)³⁴ provides a comprehensive survey of e-contract formation rules, including the time and place of contract formation through electronic means, which are directly relevant to AI-generated contracts.

Pollock and Mulla's authoritative commentary on the Indian Contract and Specific Relief Acts³⁵ remains indispensable for the interpretation of the 1872 Act's provisions, including offer, acceptance, and consideration. Avtar Singh's treatise on the Law of Contract and Specific Relief³⁶ provides the most widely cited academic analysis of the Act's requirements and their judicial interpretation. Diwan and Diwan's *Law of Contract*³⁷ offers a comprehensive review of Indian contract doctrine with contemporary case law. Saxena's commentaries on the Indian Contract Act provide granular analysis of each section that informs this dissertation's doctrinal examination.

E. *Comparative and International AI Law*

The comparative literature is extensive and rapidly expanding. In the European context, the High

³⁴Ratan Lal Basu and Rajkumar Sen, *Legal Aspects of E-Commerce in India* (Allied Publishers 2019) 44.

³⁵

³⁶Avtar Singh, *Law of Contract and Specific Relief* (13th edn, Eastern Book Company 2023) 29.

³⁷Paras Diwan and Peeyushi Diwan, *Law of Contract* (2nd edn, Allahabad Law Agency 2021) 88.

Level Expert Group on AI's Ethics Guidelines for Trustworthy AI (2019)³⁸ and the AI Act 2024³⁹ establish a regulatory model premised on risk classification, transparency requirements, and human oversight. The AI Liability Directive Proposal (2022)⁴⁰ addresses civil liability for AI-caused harm and has generated significant debate about whether fault-based or strict liability is the appropriate standard. Bandyopadhyay's 'Privity of Contract and Multi-Party AI Networks' (2023)⁴¹ analyses how the multi-layered structure of AI deployments strains classical privity rules across common-law jurisdictions.

In the Anglo-American context, the Law Commission of England and Wales has produced significant reports on digital assets⁴² and automated vehicles⁴³ that provide doctrinal models for dealing with AI-related legal novelties. The Uniform Law Commission's work on the UETA⁴⁴ explicitly addresses electronic agent contracting and provides a legislative precedent for India's reform agenda. Abbott's comparative analysis⁴⁵ synthesises American, European, and Commonwealth approaches, concluding that the most effective response to AI contracting challenges combines legislative updating of foundational contract law with sector-specific regulations and judicial development of common-law doctrine.

Garg's 'Cross-Border AI Contracts: Jurisdiction and Governing Law' (2023)⁴⁶ examines the private international law dimensions of AI-generated contracts, including choice of law and enforcement of foreign judgments in AI disputes — issues of direct relevance to Indian parties engaged in cross-border AI transactions. Chimni's 'International Law and AI: Charting

³⁸High Level Expert Group on AI, 'Ethics Guidelines for Trustworthy AI' (European Commission 2019) 13.

³⁹

⁴⁰European Commission, 'Proposal for a Directive on Adapting Non-Contractual Civil Liability Rules to AI' COM(2022) 496 final (AI Liability Directive Proposal).

⁴¹Sanchit Bandyopadhyay, 'Privity of Contract and Multi-Party AI Networks' (2023) 6 *Comparative Law Review* 44, 49.

⁴²Law Commission of England and Wales and Scottish Law Commission, 'Digital Assets: Final Report' (Law Com No 412, 2023).

⁴³Law Commission of England and Wales, 'Automated Vehicles Act 2024: Report' (Law Com No 404, 2024) 55. *Comparative reference.*

⁴⁴Uniform Law Commission, 'Automated Transactions and the Uniform Electronic Transactions Act' (ALI 2022). The Commission recommended updates to accommodate AI-generated contracts.

⁴⁵

⁴⁶Ashutosh Garg, 'Cross-Border AI Contracts: Jurisdiction and Governing Law' (2023) 9 *International Journal of Law and Information Technology* 77, 82.

New Frontiers' (2022)⁴⁷ places AI governance in the context of public international law and emerging norms, providing a framework for India's engagement with international AI governance fora. Ghosh's 'Explainability and the Right to Reasons in Automated Decision-Making' (2022)⁴⁸ examines the transparency imperative from a rights perspective, arguing that affected parties must be able to understand and challenge automated decisions that have significant legal or economic consequences.

1.8 Research Methodology

This dissertation adopts a doctrinal research methodology. Doctrinal legal research — sometimes described as 'black-letter' or 'analytical' jurisprudence — involves the systematic identification, exposition, and critical evaluation of the legal rules, principles, and standards that govern a specified area of law. It draws primarily on authoritative legal sources: legislation, delegated legislation, judicial decisions, and treaty obligations. It is distinguished from empirical legal research (which uses social-scientific methods to study law in action) and from theoretical jurisprudence (which examines the philosophical foundations of law). The doctrinal method is most appropriate for this dissertation because its core objective is to determine the current state of Indian law on AI-generated contracts and to evaluate the adequacy of that law — tasks that require close engagement with statutory text, judicial precedent, and established principles of legal interpretation.

The primary sources employed in this research include: (a) Indian legislation, principally the Indian Contract Act, 1872, the Information Technology Act, 2000, the Digital Personal Data Protection Act, 2023, the Bharatiya Sakshya Adhinyam, 2023, the Consumer Protection Act, 2019, the Competition Act, 2002, the Specific Relief Act, 1963, and sectoral regulatory instruments issued by SEBI, RBI, IRDAI, and TRAI; (b) judgments of the Supreme Court of India and the High Courts, with particular attention to decisions on electronic contracts, digital evidence, agency, and standard-form contracts; and (c) law reports and digests, including AIR, SCC, and MANU databases, as well as governmental reports and white papers.

⁴⁷BN Chimni, 'International Law and AI: Charting New Frontiers' (2022) 14 Indian Yearbook of International Law 33, 40. ⁴⁸Jayanta Ghosh, 'Explainability and the Right to Reasons in Automated Decision-Making' (2022) 3 Law, Innovation and Technology 88, 95.

The secondary sources engaged include: academic monographs and edited volumes in Indian and comparative contract law, AI law, and technology law; peer-reviewed journal articles in Indian and international law reviews; practitioner texts on electronic contracts, technology agreements, and commercial law; and policy documents from national governments and international organisations.

The comparative method is employed in Chapter V to analyse the regulatory approaches of five foreign jurisdictions. The selection of the European Union, United Kingdom, United States, Singapore, and China reflects their status as the most advanced regulatory environments for AI and commercial contracts, and their combined relevance to India as a common-law jurisdiction with significant economic ties to each of these systems. The comparative analysis is normative as well as descriptive: it not only describes what each system provides but evaluates which features are transplantable to the Indian context and which are incompatible with India's constitutional structure, developmental priorities, or administrative capacity.

The principal limitation of the doctrinal method in this context is that it cannot directly measure the practical impact of the proposed reforms or predict how courts and regulators will actually apply them. This limitation is inherent in legal scholarship rather than unique to this dissertation. A further limitation is that the AI technology landscape evolves at a pace that may outstrip the analysis: developments in large language models, autonomous AI agents, and blockchain-based smart contracts between 2024 and the time of publication may have introduced new technical possibilities not fully anticipated here. This dissertation accordingly focuses on structural doctrinal challenges that are technology-neutral in character, rather than on features specific to any particular AI architecture.

1.9 Chapterisation Scheme

The dissertation is divided into seven chapters. Chapter I (Introduction) provides the background, statement of the problem, research objectives and questions, literature review, and methodology. Chapter II (AI and Commercial Contracts: Conceptual and Regulatory Framework) examines the definition and taxonomy of AI systems relevant to commercial contracting, the evolution of automated contracting, and the existing statutory framework

under Indian law. Chapter III (Doctrinal Challenges: AI-Generated Contracts under the Indian Contract Act 1872) undertakes the central doctrinal analysis, examining how each essential element of a valid contract — offer, acceptance, consideration, competency, and free consent — is problematised by AI-generated contracting. Chapter IV (Liability, Evidence, and Dispute Resolution) analyses tortious and contractual liability for AI contracting failures, the evidentiary regime for AI-generated documents, and the adequacy of existing dispute resolution mechanisms. Chapter V (Comparative Analysis) examines the regulatory approaches of the EU, UK, USA, Singapore, and China. Chapter VI (Reform Proposals) sets out a six-pillar legislative and regulatory reform agenda for India. Chapter VII (Conclusion) summarises the principal findings, scholarly contributions, and recommendations for further research.



CHAPTER II

ARTIFICIAL INTELLIGENCE AND COMMERCIAL CONTRACTS: CONCEPTUAL AND REGULATORY FRAMEWORK

2.1 Introduction

Before engaging in doctrinal analysis, it is necessary to establish a clear conceptual foundation. The term 'artificial intelligence' encompasses an extraordinarily diverse range of technologies — from simple rule-based automation to self-learning neural networks — and this diversity has direct legal implications. The doctrinal challenges posed by a rule-based contract management system that executes pre-programmed payment terms are qualitatively different from those posed by a generative AI system that autonomously drafts and negotiates bespoke commercial agreements. This chapter therefore: (i) defines AI with precision and develops a taxonomy of AI systems relevant to commercial contracting (Section 2.2); (ii) traces the evolution of automated contracting from early EDI systems to contemporary AI-driven platforms (Section 2.3); (iii) examines the existing Indian statutory framework for electronic and automated contracts (Section 2.4); (iv) analyses the intersection of AI contracting with India's sectoral regulatory frameworks (Section 2.5); and (v) identifies the conceptual category of the 'legal personality gap' that is the foundation of the doctrinal analysis in Chapter III (Section 2.6).

2.2 Defining and Classifying AI Systems for Legal Purposes

No universally accepted legal definition of artificial intelligence exists. The EU AI Act 2024 defines an AI system as 'a machine-based system that is designed to operate with varying levels of autonomy and that may exhibit adaptiveness after deployment, and that, for explicit or implicit objectives, infers, from the input it receives, how to generate outputs such as predictions, content, recommendations, or decisions that can influence physical or virtual environments.'⁴⁹ NITI Aayog's National Strategy defines AI as 'a constellation of technologies that enable machines to act with higher levels of intelligence and emulate the human

capabilities of sense, comprehend, and act.⁵⁰ The OECD Recommendation uses functionally similar language, emphasising the capacity of AI systems to make predictions, recommendations, or decisions influencing real or virtual environments.⁵¹

For the purposes of this dissertation, the following working definition is adopted: 'Artificial Intelligence' means any computational system that uses algorithms, machine learning, neural networks, or other techniques to process inputs and generate outputs — including offers, acceptances, contractual terms, or transactional decisions — in a manner that exhibits autonomous behaviour not fully pre-programmed by its developers. This definition is deliberately functional and technology-neutral, designed to remain valid as AI architectures evolve.

The legal significance of AI taxonomy lies in the degree of human oversight exercised over AI output and the predictability of that output. Table 2.1 below sets out a five-tier taxonomy of AI systems in commercial contracting, ordered by increasing autonomy and decreasing predictability.

Table 2.1: Taxonomy of AI Systems in Commercial Contracting

Tier	Category	Characteristics	Commercial Example	Legal Predictability
1	Rule-Based Automation	Pre-programmed IF-THEN logic; no learning capacity	Invoice processing bots	High
2	Expert Systems	Knowledge base + inference engine; deterministic	Legal document review systems	High to Medium
3	Supervised ML	Trained on labelled data; pattern recognition	Credit scoring; fraud detection	Medium
4	Reinforcement Learning & Deep Learning	Learns from environment feedback; emergent behaviour	Algorithmic trading; dynamic pricing	Low to Medium

⁵⁰
⁵¹

5	Generative AI / LLMs	Foundation models; autonomous text and decision generation	AI contract drafting; autonomous negotiation agents	Low
---	----------------------	--	---	-----

The legal significance of this taxonomy is considerable. Tiers 1 and 2 represent deterministic systems whose outputs are, in principle, fully traceable to pre-programmed instructions authored by identifiable human beings. The doctrinal challenges they raise are limited: liability can generally be attributed to developers or deployers who authorised the specific rules the system applies. Tiers 3, 4, and 5, by contrast, represent probabilistic systems whose outputs emerge from statistical patterns in training data or environmental feedback. These systems may generate outputs that are not specifically authorised by, or even foreseeable to, their developers or deployers — raising fundamental questions about authority, consent, and attribution that the existing Indian legal framework is not equipped to answer.

2.3 Evolution of Automated Contracting

The history of automated contracting can be organised in three phases. The first phase, spanning roughly 1970–2000, is characterised by Electronic Data Interchange (EDI): standardised machine-readable formats for commercial documents (purchase orders, invoices, shipping notices) exchanged between the computer systems of trading partners. EDI transactions were not strictly autonomous — they executed pre-agreed terms within tightly structured protocols — but they established the principle that commercial obligations could be incurred without contemporaneous human deliberation. The Information Technology Act, 2000, was enacted in part to provide legal recognition for this category of electronic commerce.⁵²

The second phase, spanning approximately 2000–2015, is characterised by automated e-commerce: web-based systems that generate and accept contractual offers in real time in response to user inputs. Click-wrap and browse-wrap agreements proliferated during this period, generating significant litigation about formation, notice, and assent. Indian courts,

⁵²

following the general common-law approach, held that electronic acceptances are valid provided the user has adequate notice of the terms and manifests assent through an unambiguous act.⁵³ The UNCITRAL Model Law on Electronic Commerce (1996) and the United Nations Convention on the Use of Electronic Communications in International Contracts (2005) provided the international frameworks that informed the IT Act's provisions on electronic contracts.⁵⁴

The third phase, from approximately 2015 to the present, is characterised by autonomous AI contracting: systems that not only execute pre-programmed transactions but autonomously generate, negotiate, and adapt contractual terms in response to counterparty behaviour and market conditions. This phase raises qualitatively different legal challenges from its predecessors. Unlike EDI, which executed pre-agreed terms, and e-commerce automation, which presented standardised offers to human users who made choices, third-phase AI systems make judgments about what terms to offer, whether to accept proposed modifications, and how to respond to performance failures — without specific instructions from human principals in respect of those particular transactions.

Table 2.2: Sector-Wise AI Transactions in India — 2023 Estimates

Sector	Estimated Daily Transactions	AI AI-Enabled (INR Cr)	Revenue Primary AI Use Case
Capital Markets (NSE/BSE)	~800 million orders/day	~1,20,000	Algorithmic trading, order matching
Banking & Financial Services	~50 million digital loans/year	~45,000	Credit scoring, loan origination
E-Commerce	~150 million transactions/day	~2,50,000	Dynamic pricing, recommendation
Insurance	~30 million policies/year	~12,000	Automated underwriting
Logistics & Supply Chain	~20 million contracts/year	~8,500	Route optimisation, procurement

⁵³

⁵⁴UNCITRAL Model Law on Electronic Commerce (1996) art 11(2). The provision addresses electronic offer and acceptance.

Legal Technology	~500,000 documents/year	~1,200	Contract drafting, review
------------------	-------------------------	--------	---------------------------

Sources: NASSCOM AI Adoption Index 2023; RBI Annual Report 2022–23; NPCI Annual Report 2022–23; IDC India AI Spending Guide 2023; IRDAI Annual Report 2022–23.⁵⁶⁵⁷⁵⁸

2.4 The Indian Statutory Framework for Electronic and Automated Contracts

The foundational statute is the Indian Contract Act, 1872, which establishes that a contract is an agreement enforceable by law⁵⁹ and that all agreements are contracts if they are made by the free consent of parties competent to contract, for a lawful consideration and with a lawful object, and are not expressly declared void.⁶⁰ The Act does not define 'person' or 'party' in a way that includes non-human entities, and its entire conceptual architecture presupposes human contracting parties.

Section 10A of the Information Technology Act, 2000, provides that where in a contract formation, the communication of proposals, the acceptance of proposals, the revocation of proposals and acceptances, as the case may be, are expressed in electronic form or by means of an electronic record, such contract shall not be deemed to be unenforceable solely on the ground that such electronic form or means was used for that purpose.⁶¹ This provision validates electronically formed contracts but does not address the deeper question of whether the contract was formed by a human-operated system or an autonomous AI. Section 10A solves the medium problem (electronic vs paper) but not the agency problem (human vs autonomous AI actor).

⁵⁶National Payments Corporation of India, 'Annual Report 2022–23' (NPCI 2023) 14. Digital payments data.

⁵⁷

⁵⁸International Data Corporation (IDC), 'India AI Spending Guide 2023' (IDC 2023) 4.

⁵⁹

⁶⁰

⁶¹

The IT Act's Second Schedule lists categories of transactions to which Part II of the Act (which includes section 10A) does not apply, including negotiable instruments (other than cheques), trusts, wills, and powers of attorney.⁶¹ These exclusions reflect an underlying legislative judgment that certain high-stakes transactions require human deliberation rather than electronic automation — a judgment that acquires renewed significance in the AI context.

The Bharatiya Sakshya Adhinyam, 2023 (BSA 2023), which replaced the Indian Evidence Act, 1872, contains updated provisions on electronic evidence, including section 57, which replaces the former section 65B certificate requirement.⁶² These provisions have direct implications for the admissibility of AI-generated contracts as evidence, examined in detail in Chapter IV.

The Digital Personal Data Protection Act, 2023 (DPDPA) regulates the processing of 'personal data' — defined broadly to include any data about an identifiable individual⁶³ — by automated means, including AI systems. Where an AI contracting system processes personal data of the contracting party (as in personalised insurance or lending), the DPDPA's requirements of consent, purpose limitation, and data minimisation apply and interact with the contract law framework in complex ways.

Table 2.3: Traditional, Smart, and AI-Generated Contracts — Comparative Analysis

Criterion	Traditional Contract	Smart Contract	AI-Generated Contract
Formation method	Human negotiation and execution	Code deployed on blockchain; automated execution	AI autonomously drafts and may execute
Legal basis	Indian Contract Act, 1872	IT Act s 10A; Contract Act	Uncertain — s 10A partial, no AI-specific statute
Consent	Express, informed human consent	Pre-deployment consent to code logic	Ambiguous — AI may exceed deployment parameters
Modification	By mutual agreement	Limited; immutable in	AI may adapt terms

⁶¹ _____

⁶² Bharatiya Sakshya Adhinyam, 2023 (Act 47 of 2023), s 57 (replacing s 65B of the Indian Evidence Act, 1872).

⁶³

		pure form	without explicit authorisation
Evidentiary record	Paper/electronic document	Blockchain ledger	AI logs; algorithm outputs — BSA 2023 s 57 applies
Liability attribution	Parties to the contract	Developer + parties	Developer/deployer/user chain — contested

2.5 Sectoral Regulatory Context

In addition to the general contract law framework, several sector-specific regulatory bodies in India have begun to address AI-generated transactions, creating a patchwork of rules that interact with general contract law doctrine in complex ways.

SEBI's regulatory framework for algorithmic trading, articulated in its 2018 Circular on Algorithmic Trading⁶⁴, requires stockbrokers to obtain SEBI approval before deploying algorithmic trading systems. The Circular imposes obligations of risk management, audit trails, and investor protection but does not resolve the underlying contract law question of whether algorithmically generated buy/sell orders constitute valid offers and acceptances under the Indian Contract Act.

The Reserve Bank of India's Working Group on FinTech and Digital Banking⁶⁵ has recommended enhanced oversight of AI-driven lending platforms, including requirements for explainability, fairness testing, and audit trails. The RBI's Master Directions on Information Technology Governance impose obligations on banks to maintain records of algorithmic decision-making processes, with implications for both contract formation and evidence.

IRDAI's guidelines on AI and ML in insurance underwriting⁶⁶ require insurers to maintain explainable models and to ensure that AI-generated policy decisions can be reviewed and overridden by human officers. This requirement implicitly acknowledges the consent and transparency problems that this dissertation identifies as central doctrinal challenges.

⁶⁴

⁶⁵ Reserve Bank of India, 'Report of the Working Group on FinTech and Digital Banking' (RBI 2018) 34.

⁶⁶

TRAI's recommendations on data ownership and privacy in the telecom sector⁶⁷ have downstream implications for AI contracting in telecommunications: when an AI system enters into a service agreement with a consumer using that consumer's personal data as part of its decision-making process, TRAI's data protection framework overlaps with the DPDPA and with the general contract law doctrine of free consent.

2.6 The Legal Personality Gap

At the heart of all the doctrinal challenges analysed in this dissertation lies what this work terms the 'legal personality gap': the structural disconnection between the AI system that actually generates, negotiates, or executes a contract, and the legal entities (humans and corporations) that the law recognises as capable of having rights and obligations. Under Indian law, as under virtually all national legal systems, only 'persons' — natural persons and entities accorded legal personality by statute (such as companies incorporated under the Companies Act, 2013⁶⁸) — can be parties to a contract. An AI system is not a person in any legally recognised sense.

The legal personality gap creates a cascade of doctrinal difficulties. If an AI system generates an offer, who made the offer — the developer, the deployer, or the user? If an AI system accepts an offer made by a human counterparty, has a binding contract been formed, and if so, between whom? If the AI system generates contractual terms that deviate from the parameters set by its deployer, are those terms binding on the deployer? If an AI system lacks the capacity to consent, can a contract formed through its operations satisfy the free consent requirement of section 13 of the Indian Contract Act?

These questions are not merely academic. They determine, in concrete commercial disputes, whether a party is bound by a contract and whether it can obtain relief for a counterparty's breach. The legal personality gap is therefore the conceptual foundation of the doctrinal analysis in Chapter III, the liability analysis in Chapter IV, and the reform proposals in Chapter VI.

⁶⁷Telecom Regulatory Authority of India, 'Recommendations on Privacy, Security and Ownership of Data in the Telecom Sector' (TRAI 2018) 18.

⁶⁸Companies Act, 2013 (Act 18 of 2013), s 2(20). A 'company' is a company incorporated under this Act or under any previous company law, and cannot include an AI system.

CHAPTER III

DOCTRINAL CHALLENGES: AI-GENERATED CONTRACTS UNDER THE INDIAN CONTRACT ACT, 1872

3.1 Introduction

This chapter undertakes the core doctrinal analysis of the dissertation: a systematic examination of each essential element of a valid contract under section 10 of the Indian Contract Act, 1872, as applied to contracts generated by AI systems. Section 10 provides that 'all agreements are contracts if they are made by the free consent of parties competent to contract, for a lawful consideration and with a lawful object, and are not hereby expressly declared to be void.'⁶⁹ This deceptively simple formulation conceals profound difficulties when the 'party' generating the agreement is an autonomous AI system rather than a human being.

The chapter examines, in turn: the formation of offer and acceptance in AI-generated transactions (Section 3.2); the doctrine of consideration as applied to AI contracts (Section 3.3); the competency requirement and the AI legal personality problem (Section 3.4); the agency doctrine as a mechanism for attributing AI actions to human principals (Section 3.5); the free consent requirements and the opacity problem of machine learning (Section 3.6); the lawful object requirement and AI-generated bias (Section 3.7); standard-form contracts and unconscionability in AI-driven contracting (Section 3.8); and additional doctrinal challenges including privity, data consideration, and void versus voidable AI contracts (Section 3.9). The chapter concludes with a summary table (Table 3.1) mapping doctrinal challenges to proposed resolutions.

3.2 Offer and Acceptance

3.2.1 *The Offer Problem*

Section 2(a) of the Indian Contract Act defines a 'proposal' (offer) as existing 'when one person signifies to another his willingness to do or to abstain from doing anything, with a view

⁶⁹

to obtaining the assent of that other to such act or abstinence.⁷⁰ The definition employs three critical terms — 'person', 'signifies', and 'willingness' — each of which is problematised by AI-generated offers.

First, the requirement of a 'person'. As noted in Section 2.6, an AI system is not a 'person' in any legally recognised sense under Indian law. The question therefore arises whether an offer generated by an AI system is legally an offer at all, or merely an invitation to treat or a data output without legal significance. The most workable answer, consistent with section 10A of the IT Act and commercial necessity, is that the AI's output constitutes an offer by the human or corporate principal who deployed the AI for the purposes of contracting. This is effectively an agency analysis: the AI acts as agent for its deployer or user, and the deployer or user is the 'person' who made the offer. But this analysis, as Section 3.5 demonstrates, encounters serious difficulties when the AI's output exceeds the scope of authority specifically granted by the principal.

Second, the requirement of 'willingness'. Willingness connotes a volitional mental state — a desire or intention to be bound on specified terms. AI systems do not have mental states, desires, or intentions. They generate outputs based on statistical computations over training data and environmental inputs. The question of whether a computational output can be said to express 'willingness' is not merely semantic: it goes to the heart of the objectivist theory of contract, which holds that the test of offer and acceptance is objective (what a reasonable person in the position of the offeree would understand) rather than subjective (what the offeror actually intended). Indian courts have adopted the objective theory of contract formation, following the English common law tradition.⁷¹ Under the objective theory, it is possible to hold that an AI-generated offer expresses 'willingness' in the legally relevant sense — i.e., it communicates a commitment to be bound on specified terms in a manner that a reasonable offeree would understand as such — even if no actual human volition lies behind it. This is the approach implicitly adopted in US law through the UETA's electronic agent provisions.⁷²

⁷⁰

⁷¹Balbir Singh v Gurdev Singh (1988) 1 SCC 77 (SC). Standard offer-and-acceptance analysis under Indian law.

⁷²

Third, the distinction between an offer and an invitation to treat is relevant to algorithmic price displays and product listings. Under the traditional common-law rule, a display of goods with a price is merely an invitation to treat, not an offer.⁷³ Applied to e-commerce, this means that a product listing generated by an AI recommendation engine is an invitation to treat, and the consumer's decision to add the item to a virtual cart and proceed to payment constitutes the offer. This analysis preserves the traditional framework but raises new questions when the AI dynamically generates personalised prices: is a personalised offer — generated by the AI specifically for a particular consumer on the basis of that consumer's data — still merely an invitation to treat, or has it crossed into the territory of an offer because it is addressed to a specific individual? Indian courts have not definitively resolved this question.

3.2.2 *The Acceptance Problem*

Section 2(b) of the Indian Contract Act provides that a proposal is accepted when 'the person to whom the proposal is made signifies his assent thereto.'⁷⁴ When an AI system accepts an offer on behalf of its deployer, two questions arise: (i) whether the AI's computational response constitutes 'signification of assent' in the legally required sense; and (ii) whether the AI had authority to accept on behalf of the deployer.

On the first question, the same objectivist analysis applied to offers is available: if the AI's response communicates, in a manner a reasonable offeror would understand as an acceptance, a commitment to be bound on the offeror's terms, then 'assent' has been 'signified' in the legally relevant sense. The IT Act's section 10A supports this analysis by providing that contracts formed through electronic means are not invalid merely because of their electronic character.⁷⁵

On the second question, the authority of the AI to accept is governed by the law of agency, examined in Section 3.5. For present purposes, it is sufficient to note that

⁷³Savigny, *System des heutigen römischen Rechts*, Vol III (1840) 107 (trans Carl Friedrich von Savigny)—classical declaration theory of contract formation.

⁷⁴Indian Contract Act, 1872, s 2(b): 'When the person to whom the proposal is made signifies his assent thereto, the proposal is said to be accepted.'

75

UNCITRAL's Model Law on Electronic Commerce, Article 11(2), provides that, '[u]nless otherwise agreed between the originator and the addressee, a message data shall be deemed to be that of the originator if it was sent by an information system programmed by, or on behalf of, the originator to operate automatically.'⁷⁶ India has not legislatively adopted this provision, creating a gap that the proposed reforms in Chapter VI seek to address.

The mirror image rule — that acceptance must be an unconditional assent to all terms of the offer — creates additional difficulties in the context of AI negotiation systems. When two AI systems negotiate with each other, rapidly exchanging modified proposals, the question of which communication constitutes the 'last shot' that determines the terms of the contract may be impossible to determine from the transactional record. This 'battle of the forms' problem, familiar in traditional commercial contracting, is dramatically compounded when the exchange occurs between algorithms operating at machine speed.

3.3 Consideration

Section 2(d) of the Indian Contract Act defines consideration as what a promisor desires and what the promisee does or promises to do at the desire of the promisor.⁷⁷ The desirousness element — consideration must move 'at the desire of the promisor' — and the requirement of a quid pro quo are both doctrinally significant in the AI context.

The 'desirousness' requirement mirrors the 'willingness' problem in offer analysis: an AI system does not desire anything, and actions taken by a counterparty in response to an AI-generated communication may technically lack the element of being taken 'at the desire of' the promisor (if the promisor is the AI itself). The agency analysis again provides the most practical solution: the AI's desire is treated as the desire of the human principal on whose behalf it acts, so that consideration furnished by the promisee moves at the desire of the deployer, who is the legally recognised promisor.

A more novel consideration challenge arises from the increasing prevalence of data-for-services exchanges in AI-driven contracting. When a consumer provides personal

⁷⁶

⁷⁷ Indian Contract Act, 1872, s 2(d).

data in exchange for access to an AI-powered service, does the personal data constitute good 'consideration' under section 2(d)? Dalmia's analysis⁷⁸ argues affirmatively, on the grounds that personal data has measurable economic value to the platform operator, which actively desires it for the purposes of model training and targeted advertising. This argument is conceptually innovative and commercially significant — it would mean that many purportedly 'free' AI services are actually exchange contracts in which the consumer's consideration takes the form of data rather than money. The corollary would be that the platform operator's obligations (not merely its terms of service, but the contractual standards of care applicable to AI service providers) are heightened.

A further consideration challenge is raised by tokenized or cryptocurrency-denominated consideration in AI-enabled smart contracts. Where an AI system automatically releases cryptocurrency to a counterparty upon detecting performance of a specified condition, the legal status of the cryptocurrency as 'consideration' under Indian law is uncertain, given the Reserve Bank of India's position on virtual digital assets and the Supreme Court's ruling in *Internet and Mobile Association of India v Reserve Bank of India* (2020). This dissertation notes the issue but does not seek to resolve the broader cryptocurrency legal question, confining the analysis to the contract formation dimension.

3.4 Competency: The AI Legal Personality Problem

Section 11 of the Indian Contract Act provides that 'every person is competent to contract who is of the age of majority according to the law to which he is subject, and who is of sound mind, and is not disqualified from contracting by any law to which he is subject.'⁷⁹ The section presupposes that contracting parties are 'persons' with either natural legal capacity (adults of sound mind) or statutory legal capacity (companies, statutory corporations). An AI system falls into neither category.

⁷⁸

⁷⁹ Indian Contract Act, 1872, s 11.

The consequences of the competency gap are severe. Under the landmark Privy Council decision in *Mohori Bibee v Dharmodas Ghose*⁸⁰, a contract with an incompetent party is not merely voidable but void ab initio under Indian law. If this principle were applied to AI-generated contracts — on the reasoning that the AI, as the actual contracting entity, lacks competency — then every AI-generated contract would be void. This would be commercially catastrophic and is not what the legislature intended when it enacted section 10A of the IT Act. The solution most consistent with existing doctrine is to treat the AI system as an agent of a competent human or corporate principal, so that the contract is formed between the principal and the counterparty rather than between the AI and the counterparty. This preserves the competency of both contracting parties. However, as Section 3.5 demonstrates, the agency analogy has significant limitations in the AI context. A deeper solution — legislative recognition of a limited form of 'AI agency' for contracting purposes, analogous to but distinct from the agent-principal relationship — is proposed in the reform agenda in Chapter VI.

The concept of 'sound mind' in section 11 is also relevant. The Explanation to section 12 of the Indian Contract Act provides that 'a person is said to be of sound mind for the purpose of making a contract, if, at the time when he makes it, he is capable of understanding it and of forming a rational judgment as to its effect upon his interests.'⁸¹ Machine-learning systems process information and generate outputs, but they do not 'understand' contracts in the phenomenological sense, nor do they form 'judgments' about the effect of contracts on their 'interests' (since they have no interests). This reinforces the conclusion that AI systems cannot be contracting parties and must act through human principals.

3.5 Agency Doctrine and Its Limits

The law of agency — under which one person (the agent) acts on behalf of another (the principal) with legal consequences binding on the principal — provides the most workable existing doctrinal framework for AI-generated contracts. Under the Indian Contract Act's provisions on agency (ss. 182–238), the agent is a person employed to do any act for another or

⁸⁰*Mohori Bibee v Dharmodas Ghose* (1903) 30 IA 114 (PC). The Privy Council held that a contract by a minor is void ab initio in India, distinguishing the position from English law.

⁸¹

to represent another in dealings with third persons. The Indian law of agency recognises actual authority (expressly or impliedly conferred on the agent by the principal), apparent authority (created by the principal's conduct toward third parties), and ratification (retrospective adoption by the principal of an agent's unauthorised act).

Applied to AI contracting, the agency model operates as follows: the human or corporate deployer is the principal; the AI system is the 'agent'; and third parties who transact with the AI do so on the understanding that the deployer stands behind the AI's acts. The deployer's actual authority encompasses any contracts that fall within the parameters the deployer programmed into or configured for the AI system. Apparent authority extends to contracts that a reasonable third party would expect the AI to be authorised to make, given the nature of the platform on which it operates.

The agency model encounters four significant difficulties in the machine-learning context. First, actual authority: a machine-learning system may generate contractual terms that are not specifically pre-authorised by the deployer and that, indeed, the deployer could not have specifically pre-authorised because the system's behaviour is emergent rather than pre-programmed. If an AI trading algorithm enters into an unusually large contract that its parameters technically permit but that the deployer did not specifically contemplate, has the deployer actually authorised that contract? The SEBI v Rakhi Trading judgment⁸² suggests that registered stockbrokers are liable for algorithmic orders within their registered parameters, but does not address emergent ML behaviour beyond those parameters.

Second, apparent authority: apparent authority is created by the principal's representations to third parties, not by the agent's own assertions of authority. In AI contracting, third parties deal with an interface that the deployer has presented as a contracting system. The deployer's decision to present an AI system as having contracting authority creates apparent authority for transactions of the kind the system is designed to perform. But what of a generative AI system that unexpectedly offers terms radically different from its normal range? Would a reasonable third party be entitled to rely on such an offer?

Third, ratification: can a deployer ratify an AI-generated contract that exceeded the AI's actual authority? In principle, yes — ratification is available where the principal, with full

⁸²SEBI v Rakhi Trading Pvt Ltd (2018) 1 SCC 1 (SC). The Supreme Court examined liability in algorithmic trading and affirmed the responsibility of registered stockbrokers.

knowledge of what the agent has done, expressly or impliedly adopts the agent's act. But where the AI executes thousands of contracts simultaneously, the deployer may not have knowledge of individual transactions sufficient to support ratification. The practical utility of ratification as a gap-filler is therefore limited in high-volume AI contracting scenarios.

Fourth, and most fundamentally, section 182 of the Indian Contract Act defines an agent as a 'person' employed to do any act for another. If an AI system is not a 'person', it cannot technically be an 'agent' within the meaning of the Act. The agency analysis is therefore not a perfect doctrinal fit but a pragmatic extension of an existing framework — an extension that this dissertation argues requires legislative confirmation to be legally secure.⁸³

3.6 Free Consent: Opacity, Manipulation, and the Machine Learning Problem

3.6.1 *The Consent Framework under the Indian Contract Act*

Section 13 of the Indian Contract Act provides that two or more persons are said to consent when they agree upon the same thing in the same sense.⁸⁴ Section 14 requires that consent be free, defining free consent as consent not caused by coercion (s. 15⁸⁵), undue influence (s. 16⁸⁶), fraud (s. 17⁸⁷), misrepresentation (s. 18⁸⁸), or mistake (ss. 20-22⁸⁹). Contracts vitiated by coercion, undue influence, fraud, or misrepresentation are voidable at the option of the party whose consent was so caused. Contracts based on bilateral mistake of fact are void.

3.6.2 *The Opacity Problem*

Machine-learning AI systems — particularly deep neural networks and large language models — are characterised by opacity: it is generally impossible, even for their developers, to provide a complete causal explanation of why the system produced a particular output. This opacity — sometimes called the 'black-box' problem — has direct implications for the free

⁸³

⁸⁴Indian Contract Act, 1872, s 13.

⁸⁵Indian Contract Act, 1872, s 15.

⁸⁶Indian Contract Act, 1872, s 16.

⁸⁷Indian Contract Act, 1872, s 17.

⁸⁸Indian Contract Act, 1872, s 18.

⁸⁹Indian Contract Act, 1872, s 20.

consent requirement. Where an AI system generates contractual terms based on an opaque algorithmic process, the counterparty cannot fully understand the basis on which those terms were generated, and the deployer cannot fully disclose it. This raises the question of whether consent to AI-generated terms can be 'informed consent' in the sense contemplated by section 13 of the Indian Contract Act.

The Supreme Court of India's landmark decision in *KS Puttaswamy v Union of India*⁹⁰ recognised informational self-determination as a component of the fundamental right to privacy under Article 21 of the Constitution. While this decision does not directly determine the interpretation of 'free consent' under the Indian Contract Act, it provides a constitutional framework within which the consent provisions of the Act must be read. If a consumer's decision to enter an AI-generated contract is based on incomplete information about the algorithmic process that generated the contract terms — because that process is opaque by design — there is a strong argument that the constitutional right to informational self-determination has been infringed, even if a technical analysis of section 14 of the Contract Act does not find a specific vitiating factor.⁹¹

3.6.3 Algorithmic Manipulation and Undue Influence

Section 16(1) of the Indian Contract Act defines undue influence as existing where 'the relations subsisting between the parties are such that one of the parties is in a position to dominate the will of the other and uses that position to obtain an unfair advantage over the other.'⁹² Modern AI systems are increasingly capable of exploiting psychological vulnerabilities to maximise conversions or extract higher prices — a practice variously described as 'dark patterns', 'algorithmic manipulation', or 'persuasive technology'. An AI system that analyses a user's browsing history, time of interaction, emotional state (inferred from text inputs), and price sensitivity in order to present personalised offers designed to maximise the probability of acceptance may be exercising something analogous to dominance over the user's will.

⁹⁰*KS Puttaswamy v Union of India* (2017) 10 SCC 1 (SC). The nine-judge bench unanimously held that the right to privacy is a fundamental right under Article 21 of the Constitution of India.

⁹¹

⁹²

The Explanation to section 16(2) provides that 'a person who is in a position to dominate the will of another' includes a person who makes a contract with a person whose mental capacity is temporarily or permanently affected by reason of age, illness, or mental or bodily distress. An AI system that targets users in moments of particular vulnerability — late-night browsing, post-diagnosis insurance shopping, distressed financial decision-making — could be considered to be contracting with persons affected by mental or bodily distress, engaging section 16(2). This is not a fanciful argument: several consumer protection regulators in India and internationally have begun to address AI-driven dark patterns as potential violations of unfair commercial practices standards.⁹³

3.6.4 AI Hallucination and Misrepresentation

A particularly acute consent problem is posed by AI 'hallucination': the tendency of large language models to generate factually incorrect information stated with apparent confidence. When an AI contract drafting system produces a contract containing materially inaccurate representations — for example, misrepresenting the technical specifications of a product or the terms of a related regulatory licence — the question arises whether this constitutes misrepresentation within the meaning of section 18 of the Indian Contract Act.⁹⁴ Section 18 defines misrepresentation to include 'the positive assertion, in a manner not warranted by the information of the person making it, of that which is not true, though he believes it to be true.' An AI system does not 'believe' anything, but if the system presents a hallucinated fact as true, and the counterparty relies on it in entering the contract, the deployer (as principal) will be responsible for the misrepresentation on agency principles — provided the deployer knew or should have known that the AI system had a propensity to hallucinate in the relevant domain. This produces an interesting regulatory dynamic: deployers who are aware of their AI system's accuracy limitations but nonetheless deploy it in contractual contexts without adequate

⁹³

⁹⁴

safeguards may face misrepresentation liability that would have been avoided with appropriate disclosure.

3.6.5 *Mistake*

Sections 20, 21, and 22 of the Indian Contract Act address various categories of mistake.⁹⁵⁹⁶⁹⁷ Bilateral mistake of fact (s. 20) renders a contract void where both parties are under a mistake as to a matter of fact essential to the agreement. A unilateral mistake (s. 22) generally does not render a contract voidable unless it was induced by the other party. The Flash Crash of 2010 on US financial markets — when algorithmic trading systems interacted to produce a 1000-point drop in the Dow Jones in minutes, creating thousands of contracts at prices radically deviating from fair value — provides a vivid illustration of the mistake problem in AI contracting. Where two AI systems are operating under algorithmic errors or interacting in unexpected ways, generating contracts at prices or on terms that neither human principal would have chosen, the bilateral mistake analysis suggests that such contracts should be voidable or void. Indian courts have not yet grappled with this scenario, but it is only a matter of time before algorithmic errors on Indian trading platforms generate analogous disputes.

3.7 Lawful Object and AI-Generated Bias

Section 23 of the Indian Contract Act renders a contract void if its object or consideration is 'forbidden by law', 'of such a nature that, if permitted, it would defeat the provisions of any law', 'fraudulent', 'of such a nature that the court regards it as immoral', or 'opposed to public policy.'⁹⁸ AI systems trained on biased data may generate contracts that, systematically and at scale, discriminate against consumers on protected grounds — offering worse loan terms to Dalits or Adivasis, higher insurance premiums to women, or lower wages to migrant workers. Such discriminatory AI-generated contracts may violate section 23 as

⁹⁵

⁹⁶Indian Contract Act, 1872, s 21.

⁹⁷Indian Contract Act, 1872, s 22.

⁹⁸Indian Contract Act, 1872, s 23.

contracts 'opposed to public policy', as well as specific anti-discrimination provisions in employment and consumer law.

The Competition Act, 2002 is also relevant. Section 3 prohibits anti-competitive agreements, and section 4 prohibits abuse of dominant position.⁹⁹ AI-driven price coordination — where competing firms' pricing algorithms independently arrive at supra-competitive prices through parallel responses to common data inputs — raises serious section 3 concerns. The Competition Commission of India has not yet issued definitive guidance on algorithmic collusion, but the problem has been analysed by the CCI in its Market Study on E-Commerce (2020), which noted the potential for algorithmic price coordination.

3.8 Standard-Form Contracts, Adhesion, and Unconscionability

AI-generated contracts are almost invariably standard-form contracts: the counterparty has no opportunity to negotiate individual terms but must accept or reject the AI-generated package as a whole. The Supreme Court of India, in *Brojo Nath Ganguly v Shri Ram Chandra Ghosh*¹⁰⁰, established the principle that courts may strike down standard-form clauses that are unconscionable or unreasonably onerous, particularly where one party is in a position of bargain superiority. The Court held that it would be 'grossly unreasonable or unconscionable' for a party in a dominant position to impose unreasonable terms on a weaker party.

AI-driven contracting intensifies the standard-form contract problem in two respects. First, it enables hyper-personalisation of terms: the AI can generate individually tailored contracts that maximise the platform's surplus while being calibrated precisely to the counterparty's willingness to pay, leaving the counterparty with minimal consumer surplus. Each consumer may see a different contract, making collective action or legal challenge difficult. Second, AI systems can update standard terms dynamically, presenting consumers with modified agreements each time they transact, potentially without adequate notice of the changes. The doctrine of reasonable notice, which traditional Indian courts have applied to standard-form contract terms, must be adapted to accommodate algorithmically updated and personalised terms.

⁹⁹Competition Act, 2002 (Act 12 of 2003), ss 3, 4.

¹⁰⁰*Brojo Nath Ganguly v Shri Ram Chandra Ghosh* AIR 1986 SC 1768 (SC). The Supreme Court held that courts may strike down unconscionable standard form clauses.

3.9 Additional Doctrinal Challenges

3.9.1 *Privity and Multi-Party AI Networks*

The doctrine of privity of contract — under which only the parties to a contract can sue or be sued on it — creates difficulties in multi-party AI contracting networks. Where a developer creates an AI system, a platform deployer integrates it, a business uses the platform for contracting, and a consumer enters a contract through the platform, the legal relationships among these parties are complex. If the AI generates a contract that harms the consumer, the consumer's privity is with the business deployer, not with the AI developer. Yet the harm may have been caused by a defect in the AI system that was within the developer's exclusive knowledge and control. The privity doctrine, as traditionally understood in India, may deny the consumer a direct contractual remedy against the developer.¹⁰¹

3.9.2 *Void vs. Voidable AI Contracts*

The classification of defective AI-generated contracts as void or voidable has significant practical consequences. A void contract is a nullity from the outset — neither party acquires rights or incurs obligations, and parties must be restored to their original positions. A voidable contract is valid until rescinded by the party entitled to avoid it — performance rendered before avoidance is generally not recoverable. The distinction matters enormously in commercial AI contracting: if an algorithmic error generates hundreds of thousands of defective contracts before it is detected, a classification of 'void' would require unwinding all of them (possibly impractical), while 'voidable' permits the affected party to choose which contracts to affirm and which to rescind.

Indian law provides that contracts induced by fraud or misrepresentation are voidable (s. 19), contracts affected by undue influence are voidable (s. 19A), and contracts based on bilateral mistake of fact are void (s. 20). The AI context complicates these categories because the 'causing' party — the AI system — is not a legal person who can form intent, meaning that the distinction between fraudulent misrepresentation (requiring intent) and innocent

101

misrepresentation (not requiring intent) must be made at the level of the human deployer rather than the AI system itself.

Table 3.1: Summary of Doctrinal Challenges and Proposed Resolutions

ICA		Current	
Requirement	Doctrinal Challenge	Judicial/Legislative Status	Proposed Resolution
Offer (s. 2(a))	AI lacks 'willingness'; medium vs agency problem	s 10A IT Act validates medium; agency not addressed	Legislative recognition of AI electronic agents; objective theory of offer
Acceptance (s. 2(b))	AI lacks 'assent'; authority scope unclear	Partial — s 10A applies; no UNCITRAL art 11(2) equivalent	Statutory presumption that automated acceptance binds deployer
Consideration (s. 2(d))	'Desire' of AI; data as consideration uncertain	No Indian case law on data consideration	Statutory recognition of data and tokenized consideration
Competency (s. 11)	AI not a 'person'; Mohori Bibee void risk	No direct precedent; void risk unresolved	Limited AI legal agent status; deployer liability backstop
Free Consent (ss. 13-22)	Opacity problem; algorithmic manipulation; hallucination	Puttaswamy (privacy); no direct AI consent case	Explainability mandate; right to explanation; dark patterns prohibition
Lawful Object (s. 23)	Algorithmic bias; price coordination	CCI market study; no decided case	Algorithmic impact assessments; CCI AI guidelines
Standard Form / Unconscionability	Hyper-personalised terms; dynamic updating	Brojo Nath Ganguly principle applies; AI not specifically addressed	Enhanced notice requirements; judicial oversight of AI-generated standard terms

CHAPTER IV

LIABILITY, EVIDENCE, AND DISPUTE RESOLUTION

4.1 Introduction

Even where an AI-generated contract is valid and enforceable in principle, commercial parties and their legal advisers must navigate three further sets of legal challenges: (i) the attribution of liability when AI-generated contracts cause harm or fail in performance; (ii) the evidentiary framework for proving the existence, terms, and performance of AI-generated contracts; and (iii) the adequacy of existing dispute resolution mechanisms to handle the novel features of AI contract disputes. This chapter examines each of these challenges in turn.

4.2 Liability for AI-Generated Contract Failures

4.2.1 The Developer-Deployer-User Liability Chain

AI-generated contract failures typically involve multiple responsible parties: the AI developer who created and trained the system; the deployer who integrated the system into a commercial platform; and the user who interacted with the platform. Establishing liability requires determining which party's act or omission caused the harm and what standard of care applied to that party.

In tort, the foundational duty of care analysis derives from *Donoghue v Stevenson*¹⁰² and its Indian analogues. The AI developer owes a duty of care to persons who are foreseeably affected by the system's operation, including deployers and end-users. The developer's duty encompasses the obligation to design, train, and test the AI system to a standard that avoids reasonably foreseeable harm — including, in the contracting context, errors in AI-generated terms, hallucinations in representations, and algorithmic biases in pricing or eligibility decisions.

The deployer owes independent duties to its contractual counterparties and, potentially, in tort. The deployer's duty encompasses the obligation to configure, monitor, and oversee the AI system appropriately for the specific contracting context, to intervene when the system

¹⁰²*Donoghue v Stevenson* [1932] AC 562 (HL). Foundational negligence case establishing duty of care—applied by analogy to AI product liability.

generates anomalous outputs, and to ensure compliance with applicable regulatory requirements including SEBI Circular obligations¹⁰³ and IRDAI guidelines.¹⁰⁴

The user (if a business) may bear liability where it has provided incorrect parameters or instructions to the AI system, or where it has failed to review or override AI-generated outputs that a reasonable person would have found obviously defective.

4.2.2 The Black-Box Causation Problem

The central challenge in AI tort liability is causation. To establish negligence, the claimant must prove that the defendant's breach of duty caused the loss in a factual sense ('but for' causation) and in a legal sense (proximate cause or remoteness). Where the AI system's decision-making process is opaque — as is the case for deep neural networks and large language models — it may be technically impossible to trace the AI's output to a specific defect in the developer's code, training data, or the deployer's configuration. This 'black-box causation problem' effectively immunises AI developers and deployers from liability in many cases, because the claimant cannot discharge the burden of proof.

The doctrine of *res ipsa loquitur* — the thing speaks for itself — may provide partial relief. Where an AI system generates a contract containing terms so egregiously unreasonable or factually inaccurate that no properly functioning system would have produced them, *res ipsa loquitur* may permit the inference of negligence without specific proof of the defect. Indian courts have applied *res ipsa loquitur* in medical negligence cases (*Jacob Mathew v State of Punjab*, (2005) 6 SCC 1) and product liability cases, and there is no principled reason why it cannot be extended to AI-generated contract failures.

4.2.3 Product Liability

The Consumer Protection Act, 2019 provides a product liability regime that is directly applicable to AI contracting failures where the AI product is supplied to consumers.¹⁰⁵ Section 2(47) defines 'product seller' broadly to include any person who sells, distributes, leases,

¹⁰³

¹⁰⁴

¹⁰⁵Consumer Protection Act, 2019 (Act 35 of 2019), ss 2(10), 2(47).

installs, prepares, packages, labels, markets, or otherwise is involved in placing the product for commercial purpose. Section 2(10) defines 'defect' as any fault, imperfection, or shortcoming in the quality, quantity, potency, purity, or standard of a product as required by applicable law or claimed by the manufacturer.

The application of these definitions to AI systems raises interpretive questions. Is an AI contracting system a 'product' or a 'service' under the 2019 Act? The distinction matters because the liability regimes for products and services differ: products attract no-fault liability for manufacturing defects, while services attract fault-based liability for deficiencies. Most AI contracting systems are delivered as software-as-a-service (SaaS), which would suggest service rather than product classification. However, the AI model itself — the trained neural network that generates contracts — has characteristics of a manufactured product and may attract the stricter product liability standard.¹⁰⁶

Table 4.1: Liability Theories for AI Contract Failures — Comparative Analysis

Liability Theory	Standard Liability	of Causation Requirement	Indian Basis	Statutory Suitability for AI
Negligence	Reasonable care	But-for + proximate	Common law / IPC	Moderate — causation problem
Strict Product Liability	Defective product	Defect + causation	CPA 2019 ss 2(10), 2(47)	Good — if AI is 'product'
Misrepresentation	False statement + reliance	Reliance + loss	ICA ss 17-18	Good for AI hallucinations
Breach of Contract	Failure of performance	Breach + loss	ICA s 73	Standard — attribution clear
Consumer Deficiency	Inadequate service	Deficiency + harm	CPA 2019 s 2(11)	Moderate — AI service context

4.3 Evidence: AI-Generated Contracts under the Bharatiya Sakshya Adhinyam, 2023

¹⁰⁶Tanvi Bhatt, 'The Liability Puzzle: AI and Product Defects in India' (2023) 11 Journal of Indian Law and Society 44, 50.

The Bharatiya Sakshya Adhiniyam, 2023 (BSA 2023), which replaced the Indian Evidence Act, 1872 with effect from 1 July 2024, contains updated provisions on electronic evidence of direct relevance to AI-generated contracts.¹⁰⁷

Section 57 of the BSA 2023 — the successor to the much-litigated section 65B of the Indian Evidence Act — prescribes the requirements for admission of electronic records in evidence. An electronic record must be accompanied by a certificate from a person in a responsible official position in relation to the operation of the relevant device, confirming the identity of the device, the manner in which the electronic record was produced, the proper operation of the device, and the absence of tampering. For AI-generated contracts, this requirement raises practical difficulties: the 'device' generating the contract may be a distributed cloud computing infrastructure with no single 'responsible official' in the traditional sense; the 'manner in which the record was produced' may require explanation of a machine-learning model that is technically opaque; and the concept of 'tampering' is complex when the AI continually updates its model on the basis of new data.

The Supreme Court's clarification of section 65B in *Anvar PV v PK Basheer*¹⁰⁸ and *Arjun Panditrao Khotkar v Kailash Kushanrao Gorantyal*¹⁰⁹ established that the certificate requirement is mandatory for electronic records other than those produced from devices within the exclusive possession and control of the party producing them. The evolution of this requirement under the BSA 2023 must now be read in light of AI-specific challenges.

Beyond certification, AI-generated contracts present challenges of authenticity and integrity. Traditional contract authentication relies on signatures (handwritten or digital), which provide non-repudiation — the inability of the signing party to deny having executed the document. AI-generated contracts may not bear signatures in the traditional sense; they may be evidenced only by algorithmic logs, server records, and API call histories. The integrity of these records is vulnerable to post-hoc manipulation, particularly where the AI platform's logging infrastructure is under the sole control of one contracting party.

¹⁰⁷

¹⁰⁸ *Anvar PV v PK Basheer* (2014) 10 SCC 473 (SC). The Supreme Court held that electronic records require certification under s 65B of the Indian Evidence Act, 1872 before admission.

¹⁰⁹ *Arjun Panditrao Khotkar v Kailash Kushanrao Gorantyal* (2020) 7 SCC 1 (SC). The Constitution Bench clarified the procedure for admission of electronic evidence under s 65B.

4.4 Dispute Resolution Mechanisms

4.4.1 *Civil Courts and Commercial Courts*

Disputes arising from AI-generated commercial contracts are, in principle, justiciable before India's civil courts and, where they meet the pecuniary and subject-matter thresholds, before the Commercial Courts established under the Commercial Courts Act, 2015.¹¹⁰ Commercial courts have jurisdiction over 'commercial disputes' — defined broadly to include disputes arising from contracts for the supply of goods or services, partnership agreements, joint venture agreements, technology contracts, and intellectual property matters. AI-generated contracts in most commercial contexts will qualify.

However, civil litigation presents several challenges in the AI contract context. First, the technical complexity of AI systems means that litigation necessarily involves expert evidence on machine-learning architecture, training data, and algorithmic outputs — expertise that is rare among both lawyers and judges. Second, the speed of AI contracting means that by the time a dispute is filed and heard, the AI system may have been updated, modified, or decommissioned, making forensic reconstruction of the offending transaction extremely difficult. Third, the potential for algorithmic errors to affect millions of consumers simultaneously means that individual civil litigation is an inefficient dispute resolution mechanism; class action or representative proceedings would be more appropriate, but India's framework for class actions in commercial matters remains underdeveloped.

4.4.2 *Arbitration*

Arbitration under the Arbitration and Conciliation Act, 1996¹¹¹ (as amended by the 2021 Amendment Act¹¹²) is an increasingly common dispute resolution mechanism for commercial contracts in India. AI-generated commercial contracts routinely include arbitration clauses. Several issues arise specifically in the AI arbitration context.

First, the formation of the arbitration agreement: under section 7 of the Arbitration Act, an arbitration agreement must be in writing. Where the main contract is AI-generated, the

¹¹⁰Commercial Courts Act, 2015 (Act 4 of 2016), ss 2, 3, 7.

¹¹¹Arbitration and Conciliation Act, 1996 (Act 26 of 1996), s 7.

¹¹²Arbitration and Conciliation (Amendment) Act, 2021 (Act 3 of 2021).

arbitration clause it contains is also AI-generated. The question whether an AI-generated arbitration clause constitutes a valid 'written agreement' for the purposes of section 7 — given the competency and consent problems identified in Chapter III — is unresolved. The Supreme Court of India has held that an arbitration clause in an electronic contract is valid under section 7 read with section 10A of the IT Act, but the specific question of AI generation has not been addressed.

Second, the joinder of non-parties: where an AI developer's defective system has caused the harm underlying a commercial arbitration, the claimant may wish to join the developer as a respondent. But the developer is not a party to the arbitration agreement between the deployer and the counterparty, and conventional privity analysis would bar its joinder. This is a significant gap in the dispute resolution architecture for multi-party AI failures.

Third, recognition and enforcement of AI arbitration awards under the New York Convention:¹¹³ an award issued by an arbitral tribunal seated in a Convention country and arising from an AI-generated commercial contract will generally be enforceable in India under Part II of the Arbitration Act. However, an award that is tainted by an AI formation defect — where the arbitration agreement itself is void for lack of competency — may be resisted on public policy grounds under section 48(2)(b) of the Act.

Table 4.2: Dispute Resolution Mechanisms — Adequacy Assessment for AI Contract Disputes

Forum	Speed	Technical Expertise	Mass Capacity	Dispute Adequacy Rating
District Courts	Civil Low	Low	Very Low	Inadequate
Commercial Courts	Medium	Low-Medium	Low	Partially adequate
High Court (Orig. Side)	Medium	Medium	Very Low	Partially adequate
Domestic Arbitration	Medium-High	High (parties choose)	Low	Good for B2B
Consumer	Low-Medium	Low	Medium	Inadequate (technical

¹¹³Convention on the Recognition and Enforcement of Foreign Arbitral Awards (New York Convention) (1958) 330 UNTS 38.

Commissions				gap)
ODR Platform (proposed)	High	High (AI-assisted)	High	Very Good (if established)
AI Contract Disputes Tribunal (proposed)	High	Very High (specialist)	High	Excellent (if established)

4.5 Judicial Trends and Emerging Case Law

Indian courts have not yet directly adjudicated the core doctrinal questions about AI-generated contracts. However, several decisions provide important analogical precedents. *SEBI v Rakhi Trading Pvt Ltd*¹¹⁴ addressed liability in algorithmic trading and established that stockbrokers are liable for algorithmic orders placed through their registered systems, including orders that exceed normal trading patterns. This decision implicitly endorses the agency model for AI-generated securities transactions and affirms that deployers bear primary liability for algorithmic outputs.

The Puttaswamy right to privacy decision¹¹⁵ provides a constitutional framework for challenging AI contracts that involve automated processing of personal data without adequate consent or transparency. Several High Court decisions in consumer matters involving app-based service providers have applied standard unconscionability principles to app-generated contracts, finding in favour of consumers where the AI-generated terms were materially one-sided and the consumer had no meaningful opportunity to negotiate. These decisions, while not specifically addressing AI formation questions, signal a judicial disposition toward consumer-protective interpretation of AI-generated standard-form terms.

4.6 Cross-Border Jurisdiction and Governing Law

Many AI-generated commercial contracts in India involve cross-border elements: the AI developer may be a US company, the cloud infrastructure may be hosted in Singapore, the

¹¹⁴

¹¹⁵

deployer may be an Indian company, and the counterparty may be a consumer in Mumbai. The determination of governing law and jurisdictional forum is governed by the Indian private international law rules, which are not codified comprehensively and remain substantially judge-made.¹¹⁶

Indian courts generally give effect to express choice-of-law and choice-of-forum clauses in commercial contracts, following the principle of party autonomy. However, where the choice-of-law clause itself is AI-generated — and particularly where it selects a foreign law that provides significantly lower consumer protection than Indian law — courts may decline to enforce it on public policy grounds, as they have done in consumer matters under the Consumer Protection Act.¹¹⁷

The data localisation requirements of the Digital Personal Data Protection Act, 2023 add an additional dimension to cross-border AI contracting: where an AI system processes personal data of Indian citizens, certain obligations of the DPDPA apply regardless of where the developer or deployer is incorporated.¹¹⁸ This extraterritorial reach of Indian data protection law will increasingly constrain the contractual choices of foreign AI providers serving Indian markets.

¹¹⁶

¹¹⁷

¹¹⁸

CHAPTER V

COMPARATIVE ANALYSIS: INTERNATIONAL REGULATORY APPROACHES TO AI-GENERATED CONTRACTS

5.1 Introduction

No nation's legal system has yet fully resolved the challenges posed by AI-generated contracts. However, significant legislative and judicial activity in the EU, UK, USA, Singapore, and China provides comparative materials from which India can learn. This chapter analyses each jurisdiction's approach, drawing out lessons for Indian law reform. The analysis is organised around five criteria: (i) statutory recognition of AI agency; (ii) transparency and explainability requirements; (iii) liability framework for AI contracting failures; (iv) consumer protection in AI contracting; and (v) dispute resolution mechanisms. A comparative matrix (Table 5.1) provides a synoptic overview.

5.2 The European Union

The EU AI Act 2024¹¹⁹ represents the world's most comprehensive legislative response to AI and is therefore the most significant comparative reference for this dissertation. The Act adopts a risk-based approach, classifying AI systems into four categories (unacceptable risk, high risk, limited risk, and minimal risk) and imposing obligations calibrated to the risk level. AI systems used in credit scoring, insurance underwriting, employment decisions, and essential services are classified as 'high-risk' and subject to mandatory requirements of transparency (Article 13¹²⁰), human oversight (Article 14¹²¹), and technical documentation.

The Act's transparency requirements — which mandate that high-risk AI systems provide users with 'clear and understandable information' about the AI's operation — directly address the opacity problem identified in Chapter III of this dissertation. Article 22 of the EU General Data Protection Regulation (GDPR) provides individuals with the right not to be

¹¹⁹

¹²⁰ AI Act (n 4) art 13.

¹²¹ AI Act (n 4) art 14.

subject to automated decision-making that produces 'significant effects', and with the right to an explanation of automated decisions.¹²² These rights apply to AI-generated contract terms that significantly affect consumer interests, providing a precedent for India's proposed explainability mandate.

The proposed EU AI Liability Directive¹²³ would introduce a rebuttable presumption of causation in favour of AI-related claimants where the defendant has failed to comply with transparency obligations, effectively reversing the evidentiary burden in AI liability cases. This is a significant departure from traditional fault-based liability and represents the most progressive position among the comparator jurisdictions.

5.3 The United Kingdom

The UK has taken a more cautious, sector-led approach to AI regulation. The Government's Pro-Innovation White Paper (2023)¹²⁴ eschews a comprehensive AI Act in favour of principles-based guidance issued through existing sectoral regulators (FCA, ICO, CMA), complemented by cross-cutting principles of safety, transparency, fairness, accountability, and contestability. The Law Commission of England and Wales has conducted reviews of digital assets¹²⁵ and automated vehicles¹²⁶ that provide doctrinal models for dealing with AI legal novelties, but has not yet produced a comprehensive report on AI and contract law.

English courts have begun to develop common-law doctrine in AI contexts. In *R (Bridges) v Chief Constable of South Wales Police*¹²⁷, the Court of Appeal addressed the lawfulness of automated facial recognition, articulating standards of transparency and necessity that have cross-applicability to AI contracting. The Law Commission's report on

¹²²Regulation (EU) 2016/679 (General Data Protection Regulation) [2016] OJ L 119/1, art 22.

¹²³

¹²⁴UK Government, 'A Pro-Innovation Approach to AI Regulation' (White Paper, DSIT 2023) Cm 815, 9.

¹²⁵

¹²⁶

¹²⁷*R (Bridges) v Chief Constable of South Wales Police* [2020] EWCA Civ 1058. UK Court of Appeal on facial recognition—relevant to AI opacity issues.

digital assets addresses the legal status of tokens and cryptographic records — including smart contract outputs — and recommends legislative clarification of their status as property, providing a model for India's digital asset law.

5.4 The United States

US law provides the most advanced legislative recognition of AI-generated contracts among the comparator jurisdictions. The Uniform Electronic Transactions Act (UETA), enacted in 47 states, explicitly provides in section 14 that a contract may be formed by the interaction of electronic agents of the parties, even if no individual was aware of or reviewed the agents' actions or the resulting terms, and that such a contract is valid.¹²⁸ The federal E-SIGN Act contains equivalent provisions.¹²⁹ This explicit statutory recognition of electronic agent contracting resolves the offer, acceptance, and competency problems at the level of contract formation, attributing all such contracts to the human or corporate operator who deployed the electronic agent.

The American Law Institute's work on Artificial Intelligence¹³⁰ is developing principles for AI liability that draw on product liability, negligence, and warranty doctrines, adapted for the specific characteristics of AI systems. Executive Order 14110 on AI Safety¹³¹ requires federal agencies to assess AI risks and develop sector-specific guidelines, reflecting a continuing federal commitment to AI governance that complements the state-level UETA regime.

5.5 Singapore

Singapore's approach combines legislative clarity on AI contract formation with flexible, principles-based AI governance. The Electronic Transactions Act, as amended in

¹²⁸

¹²⁹E-Sign Act (Electronic Signatures in Global and National Commerce Act) 15 USC §§ 7001–7006 (2000).

¹³⁰ALI, 'Restatement of the Law, Third, Torts: Liability for Physical and Emotional Harm' (ALI 2010) as extended by ALI Principles of the Law: Artificial Intelligence (ALI 2023 Draft).

¹³¹US Executive Order 14110 on the Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence (30 October 2023) 88 Fed Reg 75191.

2021¹³², explicitly provides that a contract formed by the interaction of an electronic agent and a natural person is not void or unenforceable solely on the ground that no natural person reviewed or was aware of the agent's actions — directly solving the legal personality and competency problems that Indian law leaves unresolved.

The Model AI Governance Framework¹³³ provides detailed guidance on internal governance, human oversight, and risk management for AI systems, including contracting applications. The Framework's emphasis on explainability and auditability directly informs the disclosure and audit trail requirements proposed in Chapter VI of this dissertation.

5.6 China

China's approach to AI regulation is the most interventionist among the comparator jurisdictions. The Provisions on the Administration of Algorithmic Recommendations (2022)¹³⁴ impose obligations of transparency, opt-out rights, and anti-discrimination requirements specifically on algorithmic recommendation and pricing systems — precisely the category of AI systems that generate personalised commercial offers at scale. The Interim Measures for Generative AI Services (2023)¹³⁵ extend similar requirements to large language model-based services, requiring content accuracy, consumer protection, and regulatory review of AI-generated outputs.

The Civil Code of China (2020) contains provisions on electronic contract formation (Articles 469–491)¹³⁶ that recognise electronically formed contracts but do not specifically address AI-generated contracts. Chinese judicial practice has, however, been developing through a growing number of decisions from internet courts (established in Beijing, Shanghai, and Guangzhou), which have addressed questions of AI-generated content ownership, algorithmic recommendation liability, and electronic evidence — providing the world's richest body of judicial experience in AI-related contract disputes.

¹³²

¹³³Ministry of Justice (Singapore), 'Model AI Governance Framework' (IMDA/PDPC 2nd edn 2020) 22–30.

¹³⁴China Cyberspace Administration, 'Provisions on the Administration of Algorithmic Recommendations' (effective 1 March 2022) art 24.

¹³⁵China Cyberspace Administration, 'Interim Measures for the Administration of Generative Artificial Intelligence Services' (effective 15 August 2023) art 17.

¹³⁶People's Republic of China Civil Code (2020) arts 469–491.

Table 5.1: Comparative Regulatory Framework Matrix — AI and Commercial Contracts

Jurisdiction	AI Statutory Recognition	Agent Transparency / Explainability	Liability Standard	Consumer Protection	Specialist Dispute Forum
EU	Not explicit; AI Act risk framework	Strong — AI Act Art. 13; GDPR Art. 22	Rebuttable presumption (proposed)	Very Strong	Data Protection Authorities; courts
UK	Not explicit; sector-based	Moderate — principles-based	Fault-based; Law Commission review	Strong	FCA; ICO; courts
USA	Explicit — UETA s 14; E-SIGN	Moderate — EO 14110; sector rules	Product/negligence; ALI Principles	Strong (FTC; CFPB)	State courts; FTC; sector regulators
Singapore	Explicit — ETA s 11A	Strong — Model AI Governance Framework	Fault-based; PDPA overlay	Strong	PDPC; courts; arbitration
China	Not explicit; Civil Code art 469	Strong — Algo Recs Provisions	Fault + strict; CCP courts	Strong (CAC enforcement)	Internet courts; arbitration
India (Current)	None — IT Act s 10A partial	Weak — no AI-specific mandate	Fault-based; CPA 2019 product liability	Moderate (CPA 2019)	Civil courts; consumer forums; arbitration

5.7 Key Lessons for India

Five cross-cutting lessons emerge from the comparative analysis. First, explicit statutory recognition of AI-generated contracts is essential. The UETA and Singapore ETA models demonstrate that a single, clearly drafted statutory provision can resolve the formation problems identified in Chapter III without requiring comprehensive AI legislation. India should enact an equivalent provision as a matter of priority. Second, transparency and explainability requirements must be specific and enforceable, not merely aspirational. The EU's rights-based approach under GDPR Article 22 provides the most robust model, but it must be calibrated to India's administrative capacity. Third, the liability framework must address the causation problem. The EU's proposed rebuttable presumption — which shifts the

evidentiary burden to the AI developer where they have failed to comply with transparency obligations — is the most sophisticated solution yet proposed and merits serious consideration in the Indian context. Fourth, consumer protection must be specifically tailored to AI-generated contracts, addressing dark patterns, algorithmic manipulation, and the opacity of personalised terms. Fifth, specialised dispute resolution infrastructure is necessary: the technical complexity of AI contract disputes exceeds the competence of general civil courts and requires specialist tribunals or arbitral panels with technical expertise.

Table 5.2: Generative AI in Contract Drafting — Jurisdiction Comparison (2024)

Jurisdiction	Regulation of GenAI Contract Drafting	Disclosure Requirement	Professional Liability
EU	AI Act Art. 52 (transparency for GenAI systems)	Mandatory AI-generated content labelling	Developer + deployer liability; GPAI model rules
UK	Principles-based; FCA guidance pending	Voluntary disclosure recommended	Solicitors Act + professional rules
USA	FTC AI guidance; state law disclosure bills	Several states require AI disclosure in contracts	State bar ethics opinions; ABA guidance
Singapore	Model Framework Annex on GenAI (2023)	Recommended — Model Framework	Law Society guidance pending
India	None specific to GenAI drafting	No mandatory disclosure requirement	Bar Council of India rules; no AI guidance



CHAPTER VI

REFORM PROPOSALS: TOWARDS A COMPREHENSIVE INDIAN FRAMEWORK FOR AI-GENERATED COMMERCIAL CONTRACTS

6.1 Introduction

The doctrinal analysis in Chapter III, the liability and evidence analysis in Chapter IV, and the comparative analysis in Chapter V converge on a common conclusion: India's existing legal framework is inadequate for AI-generated commercial contracts, and reform is both necessary and urgent. This chapter sets out a six-pillar reform agenda designed to address the specific doctrinal gaps identified in this dissertation while remaining sensitive to India's constitutional structure, administrative capacity, and developmental priorities. The six pillars are: (I) legislative recognition of AI electronic agents; (II) a risk-based contract validation framework; (III) transparency and explainability mandates; (IV) a graduated liability framework; (V) enhanced evidentiary standards for AI-generated contracts; and (VI) specialist dispute resolution infrastructure.

6.2 Pillar I: Legislative Recognition of AI Electronic Agents

The most fundamental reform required is explicit statutory recognition that contracts formed by AI electronic agents are valid and binding on the human or corporate deployers of those agents. The model for this reform is the UETA section 14 in the United States¹³⁷ and section 11A of Singapore's Electronic Transactions Act.¹³⁸ In the Indian context, this reform is best implemented through an amendment to the Information Technology Act, 2000, inserting a new section 10B.

The proposed text of section 10B is as follows:

<p>Proposed Section 10B, Information Technology Act, 2000 — Contracts Formed by Artificial Intelligence Systems (1) A contract is not invalid solely because it was formed, in whole or in part, by</p>
--

¹³⁷
¹³⁸

autonomous operation of an artificial intelligence system acting on behalf of a person or entity.

(2) Where a contract is formed by an artificial intelligence system, the person or entity on whose behalf the artificial intelligence system was deployed shall be deemed to be the party to the contract for all purposes of the Indian Contract Act, 1872.

(3) For the purposes of this section, 'artificial intelligence system' means any computational system that uses algorithms, machine learning, neural networks, or equivalent techniques to generate, offer, accept, modify, or execute contractual terms on behalf of a person or entity.

(4) The person or entity on whose behalf an artificial intelligence system operates shall be responsible for ensuring that the system operates within the scope of the authority conferred by this section, and shall be liable for any breach of contract or other legal obligation arising from the system's operation.

(5) This section does not affect any other requirement of law applicable to the validity of a contract, including requirements of registration, stamp duty, or

This proposed provision resolves the offer, acceptance, and competency problems identified in Chapter III by providing a clear statutory basis for the validity of AI-generated contracts and unambiguously attributing such contracts to human or corporate deployers. It is consistent with section 10A of the IT Act (which validates electronic contracts) and supplements it by addressing the AI-specific agency problem. It is also consistent with Article 21 of UNCITRAL's Model Law on Electronic Commerce as updated in 2017, which India has not yet adopted but which represents international best practice.

6.3 Pillar II: Risk-Based Contract Validation Framework

Not all AI-generated contracts pose equal risks of formation defects, consumer harm, or systemic disruption. A uniform legal regime that treats an AI-generated invoice for office supplies the same as an AI-generated life insurance contract or employment agreement would be both over-inclusive (imposing compliance costs on low-risk applications) and under-inclusive (failing to provide adequate protection in high-risk contexts). The reform agenda therefore proposes a risk-based contract validation framework, modelled on the EU AI Act's risk classification approach.¹³⁹

139

Table 6.1 sets out the proposed risk tiers for AI-generated contracts in the Indian context:

Table 6.1: Proposed Risk-Based AI Contract Validation Framework for India

Risk Tier	Contract Category	Validation Requirements	Human Oversight	Regulatory Approval
Tier 1 (Low Risk)	Routine B2B procurement; invoice automation; logistics contracts below INR 1 lakh	Section 10B(2) attribution; electronic audit trail	Not required	Not required
Tier 2 (Moderate Risk)	Consumer e-commerce above INR 1 lakh; professional service agreements; SaaS contracts	Plain language summary of AI-generated terms; opt-out right; 24-hour review window	Post-generation review available	Not required
Tier 3 (High Risk)	Financial lending; employment contracts; insurance policies; healthcare services	Right to human review; explanation of AI decision logic; adverse action notice; BSA 2023 s 57 certificate	Mandatory human-in-the-loop before execution	Sector regulator registration of AI system
Tier 4 (Very High Risk)	Mortgage and secured lending; large-scale employment decisions; essential service contracts involving vulnerable consumers	All Tier 3 requirements + impact assessment + judicial/regulatory pre-approval for AI system deployment	Mandatory — contract void if AI alone executes	Full regulatory approval + periodic audit
Tier 5 (Prohibited)	Social credit scoring contracts; autonomous AI decisions about criminal justice; contracts exploiting minors through AI manipulation	Prohibited outright	N/A — prohibited	N/A — prohibited

6.4 Pillar III: Transparency and Explainability Mandates

The free consent problems identified in Chapter III — opacity, algorithmic manipulation,

hallucination — can be substantially mitigated by mandatory transparency and explainability requirements. This pillar proposes that the following obligations be imposed on deployers of AI contracting systems by amendment to the Information Technology Act (for general commercial contexts) and through sector-specific instruments (for regulated sectors).

First, a disclosure obligation: deployers must disclose to counterparties, at or before the point of contracting, that the contract has been generated or negotiated by an AI system, the identity of the deployer as the legally responsible party, and the nature of the AI system (tier classification under the risk framework). This disclosure requirement is modelled on the EU AI Act's Article 52 transparency obligations¹⁴⁰ and is consistent with section 18 of the Indian Contract Act's misrepresentation framework.

Second, a right to explanation: for Tier 3 and Tier 4 AI contracts, the counterparty must have a statutory right to receive, upon request, an explanation of the principal factors that led the AI system to generate the specific terms offered. This right is modelled on GDPR Article 22¹⁴¹ and addresses the opacity problem by enabling counterparties to challenge discriminatory or unreasonable AI-generated terms.

Third, an audit trail requirement: deployers must maintain immutable logs of AI-generated contracts, including the model version, training data provenance, key decision variables, and timestamp, for a period of at least five years. These logs must be producible in evidence under the BSA 2023 certification regime and must be made available to regulators on request. This requirement addresses both the evidentiary problems identified in Chapter IV and the systemic risk of AI model updates rendering past contracts unverifiable.

Fourth, a dark patterns prohibition: deployers must not use AI systems to exploit psychological vulnerabilities, create false urgency, or employ deceptive interface designs (dark patterns) in AI-generated contracting. The Central Consumer Protection Authority should be empowered to investigate and penalise dark pattern practices in AI contracting, with

¹⁴⁰ AI Act (n 4) Title III, Chapter 3 (Transparency obligations).

¹⁴¹

specific guidelines modelled on the EU's Dark Patterns Guidelines and India's existing CCPA Guidelines on Dark Patterns (2023).¹⁴²

6.5 Pillar IV: Graduated Liability Framework

The liability analysis in Chapter IV demonstrated that existing Indian tort and contract law is inadequate to address AI contracting failures, principally because of the black-box causation problem and the multi-party structure of AI deployments. This pillar proposes a graduated liability framework that: (a) assigns primary strict liability to AI developers for defects in the AI system itself; (b) assigns primary negligence liability to deployers for failures of configuration, oversight, and compliance; and (c) creates a rebuttable presumption of causation in favour of claimants where the defendant has failed to comply with the transparency and audit trail requirements of Pillar III.

The strict liability standard for AI developers is justified on the grounds that developers are best positioned to control and reduce the risk of AI system defects, that they benefit commercially from widespread deployment of their systems, and that the deterrence and compensation rationales for strict liability apply in full force. This standard is consistent with section 2(10) of the Consumer Protection Act 2019 (product defects)¹⁴³ and with the emerging international consensus reflected in the EU AI Liability Directive proposal.¹⁴⁴

The rebuttable presumption of causation — which shifts the burden of proof to the defendant where they have failed to comply with audit trail requirements — directly addresses the black-box causation problem. A claimant who can demonstrate that the AI system generated a defective contract, and that the defendant failed to maintain the records that would have enabled the causation analysis, should not bear the evidentiary cost of the defendant's non-compliance. This principle is already reflected in Indian evidence law through the doctrine of adverse inference under section 114 of the Bharatiya Sakshya Adhinyam, 2023, and could be codified specifically for AI cases.

¹⁴²

¹⁴³

¹⁴⁴

6.6 Pillar V: Enhanced Evidentiary Standards

The evidentiary challenges identified in Chapter IV — certification requirements, authenticity, and integrity of AI-generated contract records — require a specific legislative and regulatory response. This pillar proposes: (a) amendment of the BSA 2023 to provide specific certification procedures for AI-generated contracts, including requirements for model identification, training data provenance, and immutable logging; (b) establishment of a National AI Contract Register — a publicly accessible database of registered AI contracting systems maintained by the Ministry of Electronics and Information Technology, analogous to the company registries maintained by the Ministry of Corporate Affairs — that enables parties and courts to verify the identity, version, and regulatory status of the AI system used in a given contract; and (c) development of national standards for AI forensics expertise, to be published by the Bureau of Indian Standards and used to qualify AI forensic experts in commercial litigation and arbitration.

The proposed AI Contract Register addresses a fundamental problem in AI evidence: the inability of a counterparty or court to independently verify that the AI system that generated a disputed contract is the same system that the deployer claims it to be, and that it was operating in its approved configuration at the time of contracting. A public register of AI system fingerprints (cryptographic hashes of model weights and configurations) would provide an independent reference point for authentication.¹⁴⁵

6.7 Pillar VI: Specialist Dispute Resolution Infrastructure

The dispute resolution analysis in Chapter IV demonstrated that existing Indian forums — civil courts, consumer commissions, arbitral tribunals — are inadequately equipped to handle AI contract disputes because of the technical complexity involved and the potential for disputes to affect large numbers of parties simultaneously. This pillar proposes a three-component specialist dispute resolution infrastructure.

First, an AI Contract Disputes Tribunal (ACDT): a specialist adjudicatory body with jurisdiction over disputes arising from AI-generated commercial contracts above a specified

¹⁴⁵Law Commission of India, 'Report No 271: Legal Framework: Blockchain and the Law' (Government of India 2022) 45.

value threshold. The ACDT would have permanent technical members (with expertise in computer science and AI) sitting alongside legal members, and would develop specialist procedural rules for discovery and evidence in AI disputes. The ACDT could be established within the existing framework of specialised tribunals under the Tribunals Reforms Act, 2021, with appeals lying to the relevant High Court.

Second, enhanced consumer forum jurisdiction: the National Consumer Disputes Redressal Commission (NCDRC) and State Consumer Disputes Redressal Commissions should be empowered to award enhanced remedies for AI-generated consumer contract harms, including class-action style relief where the same AI system has generated defective contracts for large numbers of consumers. Technical members with AI expertise should be appointed to all three tiers of the consumer commission structure.

Third, an AI Online Dispute Resolution (AI-ODR) Platform: a technology-enabled ODR platform specifically designed for lower-value AI contract disputes (below the ACDT threshold), providing automated triage, AI-assisted mediation, and expedited adjudication. The platform would be operated under the auspices of the Ministry of Law and Justice and funded through a levy on AI contracting system operators. This proposal builds on the recommendations of the ODR Committee Report (2021) and the growing Indian ODR ecosystem.

6.8 Constitutional and Institutional Framework for Reform

The reform proposals set out above require implementation within India's constitutional framework. AI-generated contracts are primarily a matter of contract law (a Central subject under Entry 7 of the Union List) and information technology (Entry 31 of the Union List¹⁴⁶), and are therefore within the exclusive legislative competence of Parliament. The proposed amendments to the Information Technology Act, 2000 and the Bharatiya Sakshya Adhiniyam, 2023 can be enacted by Parliament without requiring state legislative concurrence.

¹⁴⁶Constitution of India, Seventh Schedule, List I (Union List), Entry 31 (posts and telegraphs, including telephones); List II (State List), Entry 26 (trade and commerce within the State).

The establishment of the AI Contract Disputes Tribunal may require constitutional examination in light of the Supreme Court's decision in *Rojer Mathew v South Indian Bank* (2019) 6 SCC 1, which subjected the Tribunals Reforms Ordinance to constitutional scrutiny. The ACDT should be designed in conformity with the principles articulated in that decision, including independence of tribunal members from executive interference.

Sectoral regulatory reform — through SEBI, RBI, IRDAI, and TRAI circulars and regulations — does not require Parliamentary action and can be implemented more rapidly. This dissertation recommends a phased approach: sectoral regulatory reform as immediate action (within 12 months), followed by legislative action on the IT Act amendments and BSA amendments (12–24 months), and establishment of the ACDT and AI-ODR platform (24–48 months).

Table 6.2: Implementation Roadmap for AI Contract Law Reform in India

Phase	Timeline	Key Reform Actions	Responsible Authority
Phase 1: Immediate	0–18 months	Sectoral AI contracting guidelines (SEBI, RBI, IRDAI, TRAI); CCPA dark patterns enforcement; Law Commission reference on AI contracts	SEBI, RBI, IRDAI, TRAI, CCPA, Law Commission of India
Phase 2: Legislative	18–36 months	IT Act amendment (s 10B); BSA 2023 amendment (AI evidence); Consumer Protection Act amendment (AI product liability); Risk Framework Notification	Parliament; MeitY; MoLJ; Consumer Affairs Ministry
Phase 3: Institutional	36–60 months	Establishment of ACDT; AI-ODR Platform launch; National AI Contract Register; BIS AI forensics standards; Mandatory AI system registration for Tier 3–4 systems	MoLJ; MeitY; BIS; National AI Mission

6.9 Judicial Creativity and Interpretive Principles

Pending legislative reform, this dissertation also proposes five interpretive principles that Indian courts can apply in adjudicating AI contract disputes within the existing legislative framework.

First, the purposive interpretation principle: courts should interpret the Indian Contract Act, 1872 purposively rather than literally, giving effect to the underlying legislative purpose of enabling the enforcement of commercial agreements while protecting weaker parties from exploitation. Applied to AI contracts, this principle supports the inference of deployer responsibility from the fact of AI deployment, rather than requiring proof of specific authorisation for each AI-generated term.

Second, the objective offeror principle: following the objective theory of contract formation adopted in English and Indian law, courts should hold that an AI-generated offer or acceptance has the legal meaning that a reasonable person in the counterparty's position would ascribe to it, regardless of the subjective (non-existent) intention of the AI system. This principle is already implicit in the case law but requires explicit articulation.

Third, the deployer responsibility presumption: courts should adopt a rebuttable presumption that the deployer of an AI contracting system is responsible for all contracts generated by that system within its operational parameters, subject to the deployer's ability to demonstrate that a specific contract was generated as a result of a counterparty's manipulation or a force majeure event. This presumption reduces the information asymmetry between the deployer (who has full access to the AI system's logs) and the counterparty.

Fourth, the transparency-weighted consent principle: courts should give weight to evidence of AI opacity, dark patterns, or inadequate disclosure when assessing whether the counterparty's consent was 'free' within the meaning of section 14 of the Indian Contract Act. Where a deployer cannot explain the basis for AI-generated terms that are materially adverse to the counterparty, courts should be willing to find a vitiating factor of the misrepresentation or undue influence variety.

Fifth, the proportionality principle in remedies: where an AI-generated contract is found to be defective, courts should fashion remedies that are proportionate to the harm and that do not unnecessarily disrupt legitimate commercial relationships. In particular, courts should prefer voidable (rather than void) classification for AI contract defects wherever possible, enabling the affected party to elect whether to affirm or rescind rather than declaring all similarly situated contracts null.

CHAPTER VII CONCLUSION

7.1 Principal Findings

This dissertation has undertaken a systematic doctrinal analysis of the legal challenges that AI-generated contracts pose under Indian law. Six principal findings emerge from this analysis.

First, AI-generated contracts do not straightforwardly satisfy the essential conditions of a valid contract under section 10 of the Indian Contract Act, 1872. The foundational requirements of offer, acceptance, consideration, competency, and free consent are each problematised by the distinctive characteristics of AI systems: the absence of legal personality, the non-existence of volition and intent, the opacity of machine-learning processes, and the emergent nature of AI behaviour that may exceed the specific parameters set by human deployers.

Second, the law of agency provides the most workable existing doctrinal framework for attributing AI-generated contracts to human or corporate principals. The deployer of an AI contracting system is the relevant principal, and the AI system operates as a limited form of agent. However, this framework is not a perfect doctrinal fit — section 182 of the Indian Contract Act requires an agent to be a 'person' — and it encounters significant difficulties when AI systems generate outputs that exceed the specific parameters of their deployment. Legislative confirmation of the agency model, through a proposed section 10B of the IT Act, is necessary to provide legal security.

Third, the opacity of machine-learning systems poses genuine challenges to the free consent requirements of sections 13–22 of the Indian Contract Act. Algorithmic manipulation, dark patterns, and AI hallucination may each constitute grounds for avoiding AI-generated contracts under existing law, and the Puttaswamy right to informational self-determination provides a constitutional backdrop that reinforces the case for mandatory transparency requirements.

Fourth, Indian evidentiary law — as updated by the Bharatiya Sakshya Adhiniyam, 2023 — requires further reform to accommodate the specific certification, authentication, and integrity challenges of AI-generated contracts. The proposed National AI Contract Register and AI forensics standards would provide the infrastructure necessary for reliable evidentiary treatment of AI contract disputes.

Fifth, a comparative analysis of the EU, UK, USA, Singapore, and China reveals that India's current legal framework is significantly less developed than those of these peer jurisdictions in respect of AI-generated contracts. The US UETA model and Singapore's ETA amendment provide the most directly applicable legislative precedents for India's statutory reform, while the EU AI Act's risk-based approach and GDPR's explainability rights provide models for

India's transparency and liability framework.

Sixth, the existing dispute resolution infrastructure — civil courts, consumer commissions, and arbitral tribunals — is inadequately equipped to handle AI contract disputes because of the technical complexity involved and the potential for algorithmic errors to affect large numbers of parties simultaneously. Specialist dispute resolution infrastructure, including an AI Contract Disputes Tribunal and an AI-ODR platform, is necessary.

7.2 Original Scholarly Contributions

This dissertation makes three original contributions to Indian legal scholarship. First, it provides the first comprehensive systematic mapping of the doctrinal adequacy of the Indian Contract Act, 1872 as applied to AI-generated contracts, revealing a series of structural gaps that have not previously been analysed in the literature with comparable depth and specificity. Second, it introduces the concept of the 'legal personality gap' as an organising analytical framework for the study of AI-generated contracts under any legal system premised on human contracting parties — a concept with cross-jurisdictional applicability. Third, it develops a specific, technically informed, and constitutionally coherent six-pillar reform agenda for Indian law that translates doctrinal analysis into actionable legislative, regulatory, and judicial proposals.

7.3 Specific Recommendations

This dissertation makes the following specific recommendations:

- (i) Parliament should amend the Information Technology Act, 2000 to insert a new section 10B providing explicit recognition of AI-generated contracts and attributing them to human or corporate deployers, substantially in the terms proposed in Chapter VI.
- (ii) Parliament should amend the Bharatiya Sakshya Adhinyam, 2023 to provide specific certification and authentication procedures for AI-generated contracts, including mandatory audit trail requirements and provision for AI forensics expert testimony.
- (iii) The Law Commission of India should be tasked with preparing a comprehensive report on AI and contract law, including draft legislation for the risk-based contract validation framework and graduated liability framework proposed in Chapter VI.
- (iv) SEBI, RBI, IRDAI, and TRAI should each issue sector-specific guidelines on AI contracting within their respective jurisdictions, implementing risk-appropriate transparency, human oversight, and audit trail requirements as an immediate measure pending legislative reform.

- (v) The Supreme Court of India should issue interpretive guidelines — through appropriate institutional mechanisms — articulating the five interpretive principles proposed in Section 6.9, providing guidance to lower courts in adjudicating AI contract disputes pending legislative reform.
- (vi) India should pursue bilateral and multilateral engagement with trading partners and international organisations — including UNCITRAL, the G20 AI governance framework, and relevant bilateral investment treaty frameworks — to develop interoperable standards for cross-border AI-generated contracts involving Indian parties.

7.4 Areas for Further Research

This dissertation has necessarily confined its analysis to the contract law dimension of AI in commercial transactions. Several important related questions are beyond its scope and merit further research. First, the question of AI-generated intellectual property — including the intellectual property rights, if any, subsisting in AI-generated contract terms — requires independent analysis in the context of the Indian Copyright Act, 1957 and the Patents Act, 1970.

Second, the criminal liability dimension of AI contracting fraud — whether a deployer who intentionally configures an AI system to generate fraudulent contracts can be prosecuted under the Bharatiya Nyaya Sanhita, 2023 — merits dedicated study. Third, the constitutional dimension of AI contracts — whether AI-driven exclusion from essential services (financial credit, insurance, employment) constitutes a violation of fundamental rights under Articles 14 and 21 of the Constitution — is a significant question for constitutional law scholarship. Fourth, the long-term question of AI legal personhood — whether, as AI systems become more autonomous and sophisticated, India should consider according a form of legal personality to AI entities for limited contracting purposes — requires empirical, comparative, and normative research that goes beyond the scope of the present doctrinal analysis.

The legal challenges of artificial intelligence in commercial contracts are among the most consequential and complex questions that Indian law will face in the coming decade. This dissertation is offered as a contribution to the scholarly conversation and policy debate that must precede effective legal reform. The goal is not to impede the transformative potential of AI but to ensure that it operates within a legal framework that is fair, transparent, and accountable — principles that are, after all, the foundations on which Indian contract law itself was built.

BIBLIOGRAPHY

A. Primary Sources

I. Indian Legislation

Indian Contract Act, 1872 (Act 9 of 1872)

Information Technology Act, 2000 (Act 21 of 2000), as amended by the Information Technology (Amendment) Act 2008

Digital Personal Data Protection Act, 2023 (Act 22 of 2023) Bharatiya Sakshya Adhiniyam, 2023 (Act 47 of 2023)

Bharatiya Nyaya Sanhita, 2023 (Act 45 of 2023)

Consumer Protection Act, 2019 (Act 35 of 2019)

Competition Act, 2002 (Act 12 of 2003)

Specific Relief Act, 1963 (Act 47 of 1963), as amended Companies Act, 2013 (Act 18 of 2013)

Commercial Courts Act, 2015 (Act 4 of 2016)

Arbitration and Conciliation Act, 1996 (Act 26 of 1996), as amended

II. Indian Case Law

Anvar PV v PK Basheer (2014) 10 SCC 473

Arjun Panditrao Khotkar v Kailash Kushanrao Gorantyal (2020) 7 SCC 1 Balbir Singh v Gurdev Singh (1988) 1 SCC 77

Bhagwati Developers Pvt Ltd v Peerless General Finance & Investment Co Ltd (2013) 9 SCC 584

Brojo Nath Ganguly v Shri Ram Chandra Ghosh AIR 1986 SC 1768

Export Credit Guarantee Corporation of India v M/s Garg Sons International (2013) 1 SCC 411

KS Puttaswamy v Union of India (2017) 10 SCC 1

M/s Spring Meadows Hospital v Harjol Ahluwalia (1998) 4 SCC 39 Mohori Bibee v Dharmodas Ghose (1903) 30 IA 114 (PC)

Nariman Bhupal Tata v Ramdas Pandurang Kale (1913) 15 Bom LR 560 Rojer Mathew v South Indian Bank (2019) 6 SCC 1

SEBI v Rakhi Trading Pvt Ltd (2018) 1 SCC 1 Shreya Singhal v Union of India (2015) 5 SCC

1

III. International and Foreign Instruments

Convention on the Recognition and Enforcement of Foreign Arbitral Awards (New York Convention) (1958) 330 UNTS 38

European Parliament, Regulation (EU) 2024/1689 of 13 June 2024 (AI Act) [2024] OJ L 2024/1689

Regulation (EU) 2016/679 (GDPR) [2016] OJ L 119/1

UNCITRAL Model Law on Electronic Commerce (1996) Uniform Electronic Transactions Act (US, 1999)

Electronic Transactions Act (Singapore, Cap 88, 2011 Rev Edn) as amended 2021 China Civil Code (2020)

China Cyberspace Administration, Provisions on the Administration of Algorithmic Recommendations (2022)

IV. Government Reports and Policy Documents

G20 New Delhi Leaders' Declaration (9–10 September 2023)

Law Commission of India, Report No 271: Legal Framework: Blockchain and the Law (2022)

Ministry of Electronics and Information Technology, India AI Mission (2024) Ministry of Finance, Economic Survey 2022–23 (2023) Vol 1

NITI Aayog, National Strategy for Artificial Intelligence (2018)

NITI Aayog, Responsible AI for All (2022)

Justice BN Srikrishna (Chair), A Free and Fair Digital Economy (Ministry of Electronics and Information Technology 2018)

Rajya Sabha Committee on Ethics, Report on Ethical Standards for AI in Public Administration (2023)

Reserve Bank of India, Report of the Working Group on FinTech and Digital Banking (2018)

SEBI, Circular on Algorithmic Trading SEBI/HO/MRD/DP/CIR/P/2018/161 (2018) IRDAI, Guidelines on Use of AI and ML in Insurance Underwriting IRDAI/LIFE/CIR/MISC/101/2023 (2023)

B. Secondary Sources

I. Books and Treatises

Abbott R, *The Reasonable Robot: Artificial Intelligence and the Law* (Cambridge University Press 2020)

Avtar Singh, Law of Contract and Specific Relief (13th edn, Eastern Book Company 2023)

Basu RL and Sen R, Legal Aspects of E-Commerce in India (Allied Publishers 2019) Chopra S and White L, A Legal Theory for Autonomous Artificial Agents (University of Michigan Press 2011)

Diwan P and Diwan P, Law of Contract (2nd edn, Allahabad Law Agency 2021) Duggal P, Cyberlaw: The Indian Perspective (Saakshar Law Publications 2020)

Hallevy G, When Robots Kill: Artificial Intelligence under Criminal Law (Northeastern University Press 2013)

Kamath N, Law Relating to Computers, Internet and E-Commerce (Universal Law Publishing 6th edn 2022)

Malik S and Malik S, Supreme Court on Information Technology (Eastern Book Company 2022)

Pollock and Mulla, The Indian Contract and Specific Relief Acts (15th edn, LexisNexis 2021)

Seth R, Technology Contracts: Drafting and Negotiating in the Digital Age (Wolters Kluwer India 2021)

Wadhwa R, Principles of Insurance Law (8th edn, Wadhwa and Company 2022)

II. Journal Articles

Ambast S, 'Contractual Liability in the Age of Artificial Intelligence: Indian Perspectives' (2023) 15 Indian Journal of Law and Technology 34

Bandyopadhyay S, 'Privity of Contract and Multi-Party AI Networks' (2023) 6 Comparative Law Review 44

Bhatt T, 'The Liability Puzzle: AI and Product Defects in India' (2023) 11 Journal of Indian Law and Society 44

Chimni BN, 'International Law and AI: Charting New Frontiers' (2022) 14 Indian Yearbook of International Law 33

Dalmia VP, 'Data as Consideration in AI Contracts: An Indian Perspective' (2023) 10 Computer Law and Security Review 1

Garg A, 'Cross-Border AI Contracts: Jurisdiction and Governing Law' (2023) 9 International Journal of Law and Information Technology 77

Ghosh J, 'Explainability and the Right to Reasons in Automated Decision-Making' (2022) 3 Law, Innovation and Technology 88

Kumar P, 'Smart Contracts and the Indian Legal Framework' (2022) 5 Indian Law Review

89

Kumar S, 'Artificial Intelligence and the Law of Agency in India' (2022) 4 Indian Law Journal 55

Lath A, 'Algorithmic Decision-Making and Consumer Rights in India' (2023) 7 Jindal Global Law Review 215

Mahaseth H, 'Regulating AI in India: Learning from Global Experiences' (2023) 12 Asian Journal of International Law 201

Mohnot D, 'Electronic Contracts and Digital Commerce: Indian Legal Landscape' (2022) 8 National Law School of India Review 111

III. International and Institutional Reports

European Commission, 'Proposal for a Directive on Adapting Non-Contractual Civil Liability Rules to AI' COM (2022) 496 final

High Level Expert Group on AI, 'Ethics Guidelines for Trustworthy AI' (European Commission 2019)

IDC, 'India AI Spending Guide 2023' (IDC 2023)

Law Commission of England and Wales, 'Digital Assets: Final Report' (Law Com No 412, 2023)

McKinsey Global Institute, 'Notes from the AI Frontier' (MGI 2019)

Ministry of Justice (Singapore), 'Model AI Governance Framework' (IMDA/PDPC 2nd edn 2020)

NASSCOM–Deloitte, 'AI Adoption Index India 2023' (NASSCOM 2023) NPCI, 'Annual Report 2022–23' (NPCI 2023)

OECD, 'Recommendation of the Council on Artificial Intelligence' OECD/LEGAL/0449 (2019)

UK Government, 'A Pro-Innovation Approach to AI Regulation' (White Paper, DSIT 2023) Cm 815

UNESCO, 'Recommendation on the Ethics of Artificial Intelligence' (UNESCO 2021) US Executive Order 14110 on AI Safety (30 October 2023) 88 Fed Reg 75191

World Bank, 'Digital India: Technology to Transform a Connected Nation' (World Bank Group 2019)

World Economic Forum, 'AI Governance: A Holistic Approach' (WEF 2019)