LEGAL LIABILITY OF ARTIFICIAL INTELLIGENCE IN INDIA: CHALLENGES AND REGULATORY FRAMEWORK

Sandal Khan, B.A. LL.B., Guru Gobind Singh Indraprastha University (GGSIPU),
New Delhi, India.

ABSTRACT

Artificial Intelligence (AI) is reshaping India's socio-economic and legal landscape across sectors as varied as healthcare, judicial administration, financial services, and autonomous transportation. While the transformative potential of AI is widely acknowledged, its deployment simultaneously generates pressing questions of legal accountability that existing Indian law is ill-equipped to resolve. The present framework consisting principally of the Information Technology Act, 2000, the Digital Personal Data Protection Act, 2023, and classical common-law doctrines of tort and product liability was conceived for a paradigm of identifiable human agency and does not adequately address the autonomous, self-adaptive character of modern AI systems. This paper employs a doctrinal and comparative methodology to interrogate the structural deficiencies of the prevailing legal order, to map the principal challenges in attributing liability for AI-induced harm, and to propose targeted legislative and institutional reforms. Comparative insights are drawn from the European Union's Artificial Intelligence Act, 2024 and the United States' sector-specific regulatory architecture. The paper contends that India urgently requires a dedicated AI liability statute anchored in a risk-tiered classification system, complemented by mandatory algorithmic impact assessments and an independent regulatory authority. Without such intervention, the promise of AI-led development risks being realised at the cost of citizens' constitutional rights to equality, privacy, and dignity.

Keywords: Artificial Intelligence, Legal Liability, Information Technology Act, Digital Personal Data Protection Act, Algorithmic Accountability, Product Liability, AI Regulation India

INTRODUCTION

The ascendancy of Artificial Intelligence as an infrastructural technology of the twenty-first century confronts legal systems worldwide with questions that classical jurisprudence was not designed to resolve. AI denotes, broadly, computational systems engineered to perform cognitive tasks including visual perception, natural language processing, autonomous decision-making, and inductive pattern recognition that would otherwise demand human intelligence.[i] In India, AI has long since transcended the experimental and now permeates critical sectors of public and private life. The National Strategy for Artificial Intelligence, published by NITI Aayog in 2018, cast India as a prospective global AI 'garage': a nation capable of designing scalable, cost-effective AI solutions for the distinctive developmental challenges of the Global South, spanning precision agriculture, preventive healthcare, personalised education, and smart urban infrastructure.[ii]

This policy ambition, however, is attended by commensurate legal risk. Autonomous vehicles may occasion fatal collisions for which no human driver can be held responsible; AI-assisted diagnostic platforms may generate erroneous clinical recommendations leading to patient injury; algorithmic credit-scoring engines may systematically disadvantage marginalised communities; and AI-enabled surveillance technologies may intrude upon the right to privacy solemnly recognised by the Supreme Court of India as a fundamental right under Article 21 of the Constitution.[iii] Each of these scenarios crystallises an identical and as-yet-unanswered legal question: when an AI system inflicts harm, which actor the algorithm's developer, its commercial deployer, the end-user, or some combination thereof bears legal responsibility?

The difficulty is not merely theoretical. Indian courts have consistently applied the foundational tort-law principle that liability attaches to a legal person: either a natural person or a juristic entity recognised by statute.[iv] Current Indian law confers no legal personality upon AI systems, and the Bharatiya Nyaya Sanhita, 2023 like the Indian Penal Code, 1860 that it supersedes requires proof of mens rea as a precondition for criminal responsibility, a threshold that machines are 5 categorically incapable of satisfying.[v] Equally, the product liability framework enacted under Chapter VI of the Consumer Protection Act, 2019 was drafted against a background of tangible, static goods and sits uneasily with AI-as-a-service models that are continuously refined through live machine learning.[vi] The resulting normative vacuum exposes injured parties to an acute access-to-justice deficit.

Against this background, this paper undertakes a systematic doctrinal and comparative examination of AI liability in India. Part II surveys the existing academic and policy literature. Part III maps the operative regulatory framework. Part IV analyses the principal liability challenges. Part V draws comparative insights from the EU and United States models. Part VI advances concrete legislative and institutional recommendations, and Part VII concludes.

LITERATURE REVIEW

Scholarly engagement with AI liability has intensified markedly since the mid-2010s, tracking the accelerating commercial deployment of machine-learning systems. In the United States, Ryan Calo's foundational analysis argued that autonomous systems possess a 'novel combination of embodiment, emergence, and social meaning' that exposes fundamental lacunae in conventional liability doctrine, particularly in relation to foreseeability and the identification of a responsible tortfeasor.[vii] Calo's framework, although rooted in American common law, has exerted a discernible influence upon comparative scholarship, including in India, where the shared common-law heritage provides ready analogical purchase.

Within Indian academic discourse, AI governance has attracted growing but still insufficiently systematic attention. Umakanth Varottil and Vikramaditya Khanna have examined the corporate governance implications of algorithmic decision-making, observing that Indian company law imposes no obligation upon boards of directors to disclose their reliance on AI in material strategic decisions a transparency deficit that undermines both shareholder accountability and sectoral regulatory oversight.[viii] The Internet and Mobile Association of India (IAMAI) advanced a 'responsible AI' framework in 2020 grounded in the principles of fairness, transparency, and human oversight; critics, however, justifiably noted that the proposal was devoid of binding enforcement mechanisms and therefore unlikely to generate meaningful compliance.[ix]

NITI Aayog's working papers on 'Responsible AI for All' (2021) articulated a principle-based architecture centred on safety, inclusivity, accountability, and data protection.[x] While intellectually valuable, these documents carry no legislative force, and their implementation has remained conspicuously uneven. The Ministry of Electronics and Information Technology (MeitY) has, since 2023, conducted rounds of multi-stakeholder consultation towards a possible AI regulatory framework, yet no legislative instrument had been introduced in Parliament as of the time of writing.[xi] This legislative inertia is itself a symptom of the

regulatory lag that characterises AI governance globally.

At the theoretical level, Jack Balkin's concept of 'information fiduciaries' has offered an influential framework for imposing trust-based obligations on AI developers towards their users, analogous to the duties owed by lawyers and doctors to clients.[xii] Lawrence Lessig's seminal insight that 'code is law' remains acutely relevant: the architectural properties of algorithmic systems themselves constitute a form of private governance that must be subjected to the discipline of democratic oversight and constitutional accountability.[xiii] Shoshana Zuboff's critique of 'surveillance capitalism' has, in turn, informed Indian debates about the compatibility of AI data-extraction practices with the constitutional right to informational privacy affirmed in Justice K.S. Puttaswamy (Retd.) v. Union of India.[xiv]

The prevailing consensus in the literature holds that conventional tort, contract, and criminal law doctrines are structurally insufficient to address AI liability, and that dedicated regulatory intervention is indispensable. Significant disagreement persists, however, regarding the preferred model: whether liability should be strict or fault-based; whether AI systems of sufficient autonomy should eventually attract some form of limited legal personality; and whether regulation should adopt a horizontal or a sector-specific form. This paper engages with these debates by anchoring the analysis in India's constitutional and statutory framework, contributing a jurisdiction-specific perspective that the existing literature has not fully developed.

LEGAL FRAMEWORK IN INDIA

India presently lacks a comprehensive, standalone statute governing Artificial Intelligence. The regulatory framework applicable to AI is consequently a mosaic of pre-existing legislation and uncodified common-law principles that require considerable interpretive creativity to extend to AI-specific circumstances. The principal components of this framework are examined seriatim below.

A. The Information Technology Act, 2000

The Information Technology Act, 2000 ('IT Act') forms the bedrock statute governing electronic commerce and cyber-related conduct in India[xv]. Section 43 establishes civil liability for unauthorised access to, and damage caused to, computer systems; Section 66 criminalises

cognate conduct where accompanied by dishonest or fraudulent intent. Of particular significance for AI platforms, Section 79 extends a conditional safe harbour to 'intermediaries' who host third-party content, provided they satisfy due-diligence obligations prescribed under the Information Technology (Intermediary Guidelines and Digital Media Ethics Code)16 Rules, 2021.[xvi] The 2021 Rules impose further obligations on 'significant socialmedia intermediaries,' including requirements of transparency reporting, content moderation mechanisms, and the appointment of grievance officers.[xvii]

The IT Act's relevance to AI liability is, however, materially constrained by its conceptual architecture. The Act was drafted against a backdrop of deliberate human misuse of computer systems; it does not contemplate the scenario in which harm originates autonomously from an AI system's own outputs. The safe harbour under Section 79 creates particular uncertainty for AI platforms: no Indian court has yet authoritatively determined whether an AI system that generates defamatory, discriminatory, or otherwise unlawful content independently qualifies as an 'intermediary' passively hosting third-party material, or whether it functions as a primary content creator, thereby attracting direct liability. The answer to this question has substantial consequences for the liability exposure of AI operators and demands urgent legislative clarification.

B. The Digital Personal Data Protection Act, 2023

The Digital Personal Data Protection Act, 2023 ('DPDPA') represents a significant, if partial, legislative advance in governing AI's data-processing functions.[xviii] The DPDPA establishes a consent-based framework regulating the collection and processing of personal data by designated 'Data Fiduciaries,' and confers upon 'Data Principals' a suite of substantive rights, including rights of access, correction, erasure, and grievance redressal.[xix] The obligations of purpose limitation and data minimisation directly constrain the manner in which AI systems may harvest and repurpose personal data as training material.

Notwithstanding these advances, the DPDPA contains a conspicuous lacuna. Unlike Article 22 of the European Union's General Data Protection Regulation (GDPR), which grants data subjects a right not to be subjected to solely automated decisions that produce significant legal or similarly consequential effects, the DPDPA contains no analogous provision.[xx] This omission is particularly consequential in the Indian context, where AI-driven automated decisions increasingly determine credit eligibility, bail recommendations, social welfare

entitlements, and insurance premiums. The absence of a right to contest or seek human review of such decisions represents a significant accountability gap that exposes vulnerable populations to unchecked algorithmic power.

C. Tort Law: Negligence and Absolute Liability

Under Indian tort law, liability in negligence is established upon proof of a duty of care, breach thereof, causation, and consequential damage the four-fold analysis derived from Donoghue v. Stevenson and consistently applied by Indian courts.[xxi] The doctrine of strict liability in Rylands v. Fletcher was significantly extended by the Supreme Court in M.C. Mehta v. Union of India, wherein the Court crafted an indigenous principle of absolute liability applicable to enterprises engaged in inherently hazardous activities, under which no defence is available to the wrongdoer.[xxii] This absolute liability doctrine is potentially applicable to high-risk AI deployments such as fully autonomous surgical robotics or autonomous weapons systems where the operator knowingly introduces an ultrahazardous technology into the environment. The challenge, however, lies in establishing causation where the AI system's internal decision-making process is opaque, rendering the causal pathway from design to harm practically unverifiable.

D. Consumer Protection Act, 2019

Chapter VI of the Consumer Protection Act, 2019 ('CPA') introduced a dedicated product liability regime imposing liability upon manufacturers, service providers, and sellers for defective products and deficient services.[xxiii] Section 84 specifies that a manufacturer incurs liability where its product suffers from a manufacturing defect, a design defect, or a failure to provide adequate instructions or warnings. AI systems marketed as consumer products or delivered as digital services could, in principle, attract liability under these provisions where the AI's output constitutes a cognisable 'defect.' However, the definitions of 'product' and 'service' in the CPA were not drafted with continuously self-updating algorithmic systems in mind, and significant interpretive uncertainty persists as to whether, for example, a software update that introduces a new AI capability alters the manufacturer's existing liability exposure.

E. Criminal Law and Other Instruments

The Bharatiya Nyaya Sanhita, 2023 ('BNS'), which has superseded the Indian Penal Code,

1860, preserves the requirement of mens rea for the vast majority of criminal offences, thereby insulating AI systems from direct criminal prosecution.[xxiv] Liability for AI-enabled crimes under the BNS would therefore attach, if at all, to the human actors who deploy or misuse the technology. Additionally, the Motor Vehicles Act, 1988 (as amended in 2019) and the nascent policy framework for testing autonomous vehicles furnish a micro-level illustration of sector-specific AI liability challenges that anticipate the broader regulatory problem.[xxv] The Securities and Exchange Board of India (SEBI) has also issued circulars governing the use of algorithmic trading systems, representing one of the few existing instances of sector-specific AI regulation in India.[xxvi]

CHALLENGES IN DETERMINING LIABILITY

A. The Attribution Problem and the Accountability Gap

The most structurally intractable challenge in AI liability is the attribution problem: the difficulty of identifying a responsible legal actor when an autonomous AI system is the proximate cause of harm. Conventional product liability doctrine envisions a linear chain of causation running from the manufacturer through the distributor to the end-user, with responsibility capable of being apportioned at each link. AI systems fundamentally disrupt this linear model. A modern large language model, for instance, may be developed by one entity, fine-tuned on domain-specific data by a second, distributed via an application programming interface (API) by a third, and ultimately utilised by a fourth with the harmful output emerging from the complex, emergent interaction of all these contributions, none of which is individually sufficient to have caused the harm.[xxvii]

Legal scholarship has characterised this diffusion of responsibility as the 'accountability gap': a structural feature of AI supply chains such that no single actor bears unequivocal accountability for the system's behaviour.[xxviii] Indian law, which requires the identification of a specific wrongdoer as a precondition for civil or criminal liability, is particularly vulnerable to this gap. Vicarious liability which extends an employer's responsibility to cover the torts of employees acting in the course of employment does not translate to AI systems that stand in no employment-like relationship with any human principal and that may act in ways neither instructed nor anticipated by their operators.

B. Algorithmic Opacity and the 'Black Box' Problem

The most commercially powerful AI systems in particular deep neural networks function as 'black boxes,' generating outputs through internal computational processes that are not legible even to their architects.[xxix] This epistemic opacity generates acute evidentiary difficulties in litigation. Demonstrating that a specific harmful AI output was the product of negligent design, as opposed to an unforeseeable emergent property of a legitimately constructed system, demands access to the model's architecture, its training datasets, and the logic embedded in its inference processes. All of these elements are routinely classified as trade secrets and shielded by intellectual property protections under Indian law.[xxx]

The resulting tension between the plaintiff's evidentiary interest in algorithmic transparency and the defendant's proprietary interest in confidentiality represents a structural dilemma. The discovery provisions of the Code of Civil Procedure, 1908 empower courts to direct the production of documents essential to the just resolution of disputes, but no Indian court has yet exercised this power to compel algorithmic disclosure. Without such precedent or, preferably, a statutory evidential framework that reverses the burden of proof in appropriate circumstances plaintiffs in AI liability cases face a practically insurmountable forensic obstacle.

C. The Question of AI Legal Personality

A philosophically contested question in AI liability jurisprudence is whether sufficiently advanced AI systems should be accorded a form of limited legal personality, analogous to the juristic personhood of incorporated companies, enabling them to hold assets, bear obligations, and be subjected directly to legal process.[xxxi] The Madras High Court's observation in Balu Chokkalingam v. State of Tamil Nadu that the legislature may in future need to address the question of AI's legal status reflects nascent judicial awareness of the issue, albeit without constituting a binding precedent.[xxxii] The European Parliament's 2017 Resolution on Civil Law Rules on Robotics ultimately rejected electronic personality in favour of human-centred accountability norms a position that is persuasively applicable to India, given the constitutional primacy of human dignity enshrined in Article 21 and the expansive reading of fundamental rights by the Supreme Court.

D. Bias, Discrimination, and Fundamental Rights

AI systems trained on historically skewed datasets have been empirically demonstrated to replicate and amplify pre-existing patterns of discrimination along axes of race, gender, caste,

religion, and socioeconomic class. In India, where structural caste discrimination remains a social reality, the deployment of AI in hiring, credit assessment, law enforcement, and judicial decision-support raises acute concerns under Articles 14 and 15 of the Constitution, which guarantee equality before the law and prohibit discrimination on specified grounds respectively.[xxxiii] The Supreme Court's expansive reading of Article 21 to encompass the right to live with dignity affirmed in Francis Coralie Mullin v. Administrator, Union Territory of Delhi further sustains the argument that AI-generated discriminatory harm may constitute a constitutional tort actionable before the High Courts under Article 226.[xxxiv]

The deployment of Facial Recognition Technology (FRT) by several State police forces reportedly without any legislative authorisation, judicial oversight, or independent audit provides a concrete illustration of these constitutional risks. Documented studies, including the Internet Freedom Foundation's Project Panoptic, have identified significantly elevated false-positive rates for individuals from lower-caste and minority communities, raising the spectre of wrongful arrest, custodial harm, and institutionalised stigmatisation.[xxxv]

E. Causation in Autonomous and Self-Learning Systems

The standard 'but for' test of causation asking whether the harm would have materialised absent the defendant's breach is difficult to apply to AI-induced harm where the system operates autonomously and its decision-making cannot be fully anticipated by any human actor.[xxxvi] This challenge is compounded in reinforcement-learning systems that continuously modify their own behavioural parameters through interaction with their operating environment, potentially diverging substantially from the objectives specified at deployment. Where the harmful behaviour emerges from post-deployment learning rather than any specific design or deployment decision, the causal nexus between human conduct and harm dissolves to a degree that conventional tort analysis cannot readily accommodate.

COMPARATIVE PERSPECTIVE

A. The European Union: The AI Act and the AI Liability Directive

The European Union has developed the most comprehensive and legally binding regulatory framework for AI yet adopted by any major jurisdiction. The EU Artificial Intelligence Act, which entered into force on 1 August 2024, classifies AI systems according to four risk tiers unacceptable, high, limited, and minimal and imposes graduated regulatory obligations at each

level.[xxxvii] High-risk AI systems, including those deployed in employment recruitment, educational assessment, law enforcement, and critical infrastructure management, are subject to rigorous pre-deployment conformity assessments, mandatory human oversight mechanisms, logging and transparency obligations, and post-market monitoring requirements. AI systems posing unacceptable societal risks such as real-time remote biometric surveillance in public spaces, social scoring by public authorities, and subliminal manipulation of human behaviour are categorically prohibited.

The proposed EU AI Liability Directive complements the AI Act by harmonising member states' civil liability rules.[xxxviii] Its central innovation is a rebuttable presumption of causal linkage: where a claimant can establish that an AI system violated an applicable legal obligation and that a causal connection between the violation and the damage is plausible, the burden shifts to the AI operator to disprove causation. This evidential mechanism directly addresses the 'black box' problem by placing the burden of algorithmic explication on the party best placed to bear it the operator with access to the system's technical specifications and decision logs.

B. The United States: Sectoral Regulation and Executive Instruments

The United States has pursued a characteristically fragmented approach to AI governance, leveraging existing agency authority rather than enacting comprehensive federal legislation. The Federal Trade Commission has applied its statutory authority under Section 5 of the Federal Trade Commission Act to challenge unfair and deceptive AI practices, including the non-disclosure of AI-generated content and manipulative algorithmic design.[xxxix] The Equal Employment Opportunity Commission has issued technical guidance on the application of Title VII and the Americans with Disabilities Act to AI-assisted hiring tools. President Biden's Executive Order 14110 of October 2023 on the Safe, Secure, and Trustworthy Development and Use of AI directed federal agencies to develop sector-specific AI standards, safety evaluations, and procurement criteria, though its subsequent partial revocation underscores the political vulnerability of regulatory frameworks that rely on executive fiat rather than legislative mandate.[xl]

For India, the comparative analysis yields a twofold lesson. The EU model demonstrates the feasibility and coherence of horizontal, risk-tiered AI legislation with well-defined liability attribution rules. The US experience, conversely, illustrates the regulatory fragmentation and

legal uncertainty that attend a purely sector-specific approach in the absence of an overarching legislative framework. India's federal constitutional structure, combined with the concurrent-list status of most AI-relevant subject matters, strongly favours the adoption of a central framework statute supplemented by sector-specific delegated legislation issued by competent regulatory authorities.

SUGGESTIONS AND RECOMMENDATIONS

On the basis of the foregoing doctrinal and comparative analysis, the following legislative and policy reforms are commended for the consideration of Indian policymakers and legislators.

1. Enact a Dedicated AI Regulation and Liability Act.

India should enact a standalone Artificial Intelligence Regulation and Liability Act that: (i) establishes a risk-tiered classification system for AI applications, modelled on the EU AI Act; (ii) defines the liability obligations of developers, deployers, and users at each risk level; (iii) creates a statutory cause of action for AI-induced harm; and (iv) incorporates a rebuttable presumption of causation in favour of injured plaintiffs, drawing on the EU AI Liability Directive's evidential mechanism. The statute should further prescribe mandatory pre-deployment conformity assessments for high-risk AI systems and establish minimum transparency and logging requirements.[xli]

2. Establish an Independent AI Regulatory Authority.

A dedicated, multi-stakeholder AI Regulatory Authority should be constituted under the proposed statute. Its mandate should encompass: the certification of high-risk AI systems prior to deployment; continuous post-market surveillance; the investigation and adjudication of AI-related complaints; and the issuance of binding technical standards and interpretive guidance. The Authority should be structurally insulated from line ministerial direction to guard against regulatory capture, a persistent pathology in Indian financial and telecommunications regulation.[xlii]

3. Amend the DPDPA to Incorporate Automated-Decision Protections.

The Digital Personal Data Protection Act, 2023 should be amended to introduce a right against solely automated decision-making producing significant effects upon individuals, consistent

with the model provided by Article 22 of the GDPR. The amendment should require Data Fiduciaries deploying automated decision systems in high-stakes contexts credit, employment, healthcare, bail, and social welfare to provide an intelligible explanation of the decision and to afford individuals the right to request review by a qualified human decision-maker.[xliii]

4. Mandate Algorithmic Impact Assessments.

Entities proposing to deploy AI in high-risk contexts should be required by law to conduct and publicly disclose Algorithmic Impact Assessments ('AIAs') prior to deployment. AIAs should systematically identify foreseeable harms to fundamental rights and propose mitigation measures. This obligation should initially be incorporated into the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021 as an additional due-diligence requirement, pending enactment of the proposed AI statute.[xliv]

5. Strengthen Access to Justice for AI-Induced Harms.

Given the technical complexity and financial asymmetry characteristic of AI liability claims, dedicated access-to-justice mechanisms are essential. The government should fund AI literacy training for the judiciary and establish specialised AI tribunal benches with technical assessors. Legal aid under the Legal Services Authorities Act, 1987 should be formally extended to cover AI liability claims brought by economically disadvantaged litigants.[xlv] Additionally, consideration should be given to facilitating collective redress mechanisms, such as representative actions, for AI-induced harms affecting a class of similarly situated individuals.[xlvi]

CONCLUSION

The proliferation of Artificial Intelligence across India's economic and public institutions constitutes an unprecedented regulatory challenge that the existing legal framework is structurally unprepared to meet. The core attributes of advanced AI autonomy in decision-making, opacity of internal process, and the diffusion of responsibility across multi-layered supply chains collectively undermine a legal architecture premised upon identifiable human agency, foreseeable harm, and singular attribution of fault. The Information Technology Act, 2000, the Digital Personal Data Protection Act, 2023, and the Consumer Protection Act, 2019, while providing fragmentary protections, are individually and collectively insufficient to

address the full spectrum of AI-induced legal injury.

The comparative experience of the European Union illuminates a viable regulatory pathway: horizontal, risk-tiered legislation that classifies AI systems by their potential for societal harm, imposes proportionate ex ante and ex post obligations, and introduces targeted evidential innovations such as the rebuttable presumption of causation to address the unique forensic challenges of AI litigation. India, as a common-law jurisdiction equipped with a constitutionally entrenched fundamental rights framework and one of the world's most dynamic AI sectors, is uniquely positioned to develop a regulatory model that synthesises international best practices with the distinctive requirements of its constitutional order and development context.

The foregoing analysis identifies five immediate reform priorities: the enactment of a dedicated AI Regulation and Liability Act; the establishment of an independent AI Regulatory Authority; the amendment of the DPDPA to introduce automated decision-making protections; the mandating of Algorithmic Impact Assessments; and the strengthening of access-to-justice mechanisms for AI-related claims. Implemented cohesively, these measures would equip India's legal system to govern AI in a manner that upholds the constitutional commitments to equality, dignity, and the rule of law.

The regulation of AI is ultimately a normative undertaking that reflects a polity's judgment about the proper relationship between technological capability and human values. India's legal community its legislators, judges, practitioners, and scholars bears a collective responsibility to meet this moment with theurgency, analytical rigour, and constitutional fidelity that it demands.

Footnotes and References

i. Stuart J. Russell & Peter Norvig, *Artificial Intelligence: A Modern Approach* 1–5 (4th ed., Pearson 2020).

ii. NITI Aayog, *National Strategy for Artificial Intelligence #AIforAll* 5–9 (June 2018), https://niti.gov.in/sites/default/files/2023-03/National-Strategy-for-Artificial-Intelligence.pdf [hereinafter NITI Aayog NSAI].

iii. Justice K.S. Puttaswamy (Retd.) v. Union of India, (2017) 10 SCC 1, ¶¶ 249–267 (Chandrachud, J.) (recognising the right to privacy as a fundamental right under Art. 21 of the Constitution of India).

iv. *See* Salomon v. Salomon & Co. Ltd., [1897] AC 22 (HL) (establishing the principle of separate legal personality); *cf.* Companies Act, No. 18 of 2013, § 9 (India) (conferring juristic personality upon registered companies from the date of incorporation).

v. Bharatiya Nyaya Sanhita, No. 45 of 2023, §§ 13–15 (India) (general exceptions from criminal liability); Indian Penal Code, No. 45 of 1860, §§ 76–106 (India) (now largely superseded).

vi. Consumer Protection Act, No. 35 of 2019, §§ 82–87 (India) [hereinafter CPA 2019].

vii. Ryan Calo, *Robotics and the Lessons of Cyberlaw*, 103 Calif. L. Rev. 513, 531–535 (2015). *See also* Matthew U. Scherer, *Regulating Artificial Intelligence Systems: Risks, Challenges, Competencies, and Strategies*, 29 Harv. J.L. & Tech. 353, 358–362 (2016).

viii. Umakanth Varottil & Vikramaditya Khanna, *Algorithmic Governance and Corporate Law in India*, 12 Indian J.L. & Tech. 45, 61–68 (2021).

ix. Internet and Mobile Association of India (IAMAI), *Responsible AI Policy Framework for India* 3–7 (2020).

x. NITI Aayog, *Responsible AI for All: Adopting the Framework A Use Case Approach on Facial Recognition Technology* 11–25 (2021). *See also* NITI Aayog, *Principles for Responsible AI* (2021) (articulating eight core principles for trustworthy AI deployment in India).

xi. Ministry of Electronics and Information Technology (MeitY), *India's Approach to AI Regulation Consultation Paper* (2023). As of the date of this paper, no legislative bill on AI had been introduced in Parliament.

xii. Jack M. Balkin, *Information Fiduciaries and the First Amendment*, 49 U.C. Davis L. Rev. 1183, 1196–1212 (2016). *See also* Lina M. Khan & David E. Pozen, *A Skeptical View of Information Fiduciaries*, 133 Harv. L. Rev. 497, 510–518 (2019) (offering a critical

assessment of the fiduciary framework).

xiii. Lawrence Lessig, *Code: Version 2.0* 1–8, 120–135 (Basic Books, 2d ed. 2006).

xiv. Justice K.S. Puttaswamy (Retd.) v. Union of India, (2017) 10 SCC 1; *see also* Shoshana Zuboff, *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power* 7–18 (PublicAffairs 2019).

xv. Information Technology Act, No. 21 of 2000 (India) [hereinafter IT Act].

xvi. IT Act §§ 43, 66, 79; Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, Rule 3 (due-diligence obligations for intermediaries) [hereinafter Intermediary Guidelines Rules, 2021].

xvii. Intermediary Guidelines Rules, 2021, Rule 4(2) (additional obligations on significant social media intermediaries, including monthly compliance reports and proactive content monitoring).

xviii. Digital Personal Data Protection Act, No. 22 of 2023 (India) [hereinafter DPDPA]. *See also* Srikrishna Committee, *A Free and Fair Digital Economy: Protecting Privacy, Empowering Indians Report of the Committee of Experts on a Data Protection Framework for India* (July 2018) (providing the legislative background to the DPDPA).

xix. DPDPA §§ 6–7 (lawful grounds for processing and consent), §§ 12–13 (rights of Data Principals, including rights of access, correction, erasure, and grievance redressal).

xx. Council Regulation (EU) 2016/679 of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data, art. 22, 2016 O.J. (L 119) 1 (EU) [hereinafter GDPR] (prohibiting solely automated individual decision-making that produces significant effects, absent explicit consent or contractual necessity, with human review available on request).

xxi. Donoghue v. Stevenson, [1932] AC 562 (HL) (Lord Atkin's neighbourhood principle); Jacob Mathew v. State of Punjab, (2005) 6 SCC 1, 16–18 (Supreme Court of India applying the Donoghue test in a medical negligence context and requiring proof of duty, breach, causation, and damage).

xxii. M.C. Mehta v. Union of India, (1987) 1 SCC 395 (Bhagwati, C.J.) (formulating the doctrine of absolute liability for enterprises engaged in inherently hazardous activities, rejecting the exceptions available under Rylands v. Fletcher); *cf.* Rylands v. Fletcher, (1868) LR 3 HL 330 (establishing strict liability for non-natural use of land). *See also* Charan Lal Sahu v. Union of India, (1990) 1 SCC 613 (affirming M.C. Mehta in the Bhopal Gas litigation context).

xxiii. CPA 2019, Ch. VI, §§ 82–87 (product liability definitions, grounds of liability, and

defences available to manufacturers, service providers, and sellers).

xxiv. Bharatiya Nyaya Sanhita, No. 45 of 2023, § 13 (India) (general exception of act of a person of unsound mind; *by analogy*, AI systems, lacking any mental state, fall outside the scope of criminal liability).

xxv. Motor Vehicles (Amendment) Act, No. 32 of 2019 (India); Ministry of Road Transport and Highways, *Policy Framework for Testing of Autonomous Vehicles in India* (2020).

xxvi. Securities and Exchange Board of India (SEBI), *Circular on Framework for Algorithmic Trading*, SEBI/HO/MRD/DP/CIR/P/2016/7 (Jan. 7, 2016) (prescribing risk controls, audit trails, and kill-switch requirements for algorithmic trading systems).

xxvii. Frank Pasquale, *The Black Box Society: The Secret Algorithms That Control Money and Information* 58–72 (Harvard Univ. Press 2015). *See also* Finale Doshi-Velez et al., *Accountability of AI Under the Law: The Role of Explanation* (Berkman Klein Ctr. Research Publ'n No. 2017-19, Nov. 2017).

xxviii. Brent Mittelstadt et al., *The Ethics of Algorithms: Mapping the Debate*, 3(2) Big Data & Soc'y 1, 6–9 (2016).

xxix. Pasquale, *supra* note 27, at 3–12. *See also* Will Douglas Heaven, *Why Deep-Learning AIs Are So Easy to Fool*, MIT Technology Review (Oct. 9, 2019).

xxx. Patents Act, No. 39 of 1970, § 3(k) (India) (excluding mathematical methods, business methods, and computer programs *per se* from patentability); Copyright Act, No. 14 of 1957, § 2(o) (India) (defining 'literary work' to include computer programmes, which may protect source code as a trade secret where unpublished).

xxxi. Shyamkrishna Balganesh, *Copyright and the Protection of AI Outputs in India*, 14 Indian J.L. & Tech. 1, 18–23 (2023). *See also* European Parliament Resolution of 16 February 2017 on Civil Law Rules on Robotics, 2015/2103(INL), ¶ 59(f) (entertaining but ultimately declining to recommend electronic personality for autonomous robots).

xxxii. Balu Chokkalingam v. State of Tamil Nadu, W.P. No. 24297 of 2019 (Madras H.C.) (observing *per curiam* in *obiter dicta* that legislative guidance may be needed on the legal status of AI entities; no definitive ruling on AI personhood was issued).

xxxiii. India Const. arts. 14, 15 (guaranteeing equality before law and prohibiting discrimination on grounds of religion, race, caste, sex, or place of birth respectively).

xxxiv. Francis Coralie Mullin v. Administrator, Union Territory of Delhi, (1981) 1 SCC 608, ¶ 8 (Bhagwati, J.) (holding that Art. 21 encompasses the right to live with dignity and all that goes along with it). *See also* Navtej Singh Johar v. Union of India, (2018) 10 SCC 1, ¶ 92 (reaffirming dignity as the foundational value of the Constitution).

xxxv. Internet Freedom Foundation, *Project Panoptic: Mapping the Use of Facial Recognition Technology in India* (2021), https://panoptic.in (documenting the deployment of FRT by over twenty police forces without legislative sanction, and recording elevated error rates for minority and lower-caste individuals).

xxxvi. Barnett v. Chelsea & Kensington Hospital Management Committee, [1969] 1 QB 428 (articulating the 'but for' test of factual causation); *cf.* Spring Meadows Hospital v. Harjol Ahluwalia, (1998) 4 SCC 39 (applying causation analysis in a medical negligence claim before the Supreme Court of India).

xxxvii. Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 Laying Down Harmonised Rules on Artificial Intelligence and Amending Certain Union Legislative Acts (Artificial Intelligence Act), 2024 O.J. (L, 2024/1689) 1 [hereinafter EU AI Act].

xxxviii. Proposal for a Directive of the European Parliament and of the Council on Adapting Non-Contractual Civil Liability Rules to Artificial Intelligence (AI Liability Directive), COM(2022) 496 final (Sept. 28, 2022) [hereinafter AI Liability Directive Proposal]. *See also* European Parliament, *Report on Artificial Intelligence in a Digital Age*, 2020/2266(INI) (May 3, 2022).

xxxix. Federal Trade Commission Act, 15 U.S.C. § 45 (2018) (prohibiting unfair or deceptive acts or practices in or affecting commerce); Federal Trade Commission, *Aiming for Truth, Fairness, and Equity in Your Company's Use of AI* (Apr. 19, 2021), https://www.ftc.gov/business-guidanc e/blog/2021/04/aiming-truth-fairness-equity-your-companys-use-ai.

xl. Exec. Order No. 14,110, 88 Fed. Reg. 75,191 (Oct. 30, 2023) (Biden, Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence). Parts of the Order were subsequently revoked by Exec. Order No. 14,179 (Trump, Jan. 20, 2025).

xli. For a detailed proposal for an Indian AI liability statute drawing on the EU AI Act model, *see* Arindrajit Basu et al., *Governing AI in India: A Framework for Legislation*, Centre for Internet & Society (CIS) Working Paper (2022).

xlii. On regulatory capture in Indian financial markets, *see* Pratip Kar, *Regulatory Capture and SEBI: Conceptual Issues*, 48(8) Econ. & Pol. Wkly. 18, 20–24 (2013).

xliii. GDPR, *supra* note 20, art. 22 (right not to be subject to solely automated individual decision-making; right to obtain human intervention, express one's point of view, and contest the decision).

xliv. Intermediary Guidelines Rules, 2021, *supra* note 16, Rule 4 (existing due-diligence

framework, which could be extended by amendment to encompass pre-deployment Algorithmic Impact Assessments). *See also* Algorithmic Accountability Act of 2022, S. 3572, 117th Cong. (2022) (U.S.) (proposing mandatory impact assessments for automated decision systems, as an instructive comparative model).

xlv. Legal Services Authorities Act, No. 39 of 1987 (India) (establishing the framework for free legal services to eligible persons; the schedule of eligible categories should be amended to expressly include victims of AI-induced harm).

xlvi. *See* Code of Civil Procedure, No. 5 of 1908 (India), Or. 1, R. 8 (representative suits, permitting one or more persons to sue on behalf of all persons having the same interest, which could serve as a vehicle for collective redress in mass AI harm scenarios). *See also* Consumer Protection Act, No. 35 of 2019, § 35(1)(c) (India) (permitting class complaints before Consumer Commissions)