Ianna Journal of Interdisciplinary Studies, EISSN: 2735-9891

Volume 7, Issue 2, 2025

BETWEEN INNOVATION AND ILLEGALITY: A CRITICAL STUDY OF ARTIFICIAL INTELLIGENCE CRIMES AND THE LIMITS OF INDIA'S EXISTING PENAL AND REGULATORY REGIME

Priya Bairagi, Research Scholar, Jamnalal Bajaj School of Legal Studies, Banasthali Vidyapith

Dr. Asha Rawat, Assistant Professor, Jamnalal Bajaj School of Legal Studies, Banasthali Vidyapith

ABSTRACT

The rapid proliferation of Artificial Intelligence (AI) technologies has fundamentally transformed the nature of crime, governance, and legal accountability. While AI-driven innovation offers significant economic and administrative benefits, it simultaneously enables novel forms of criminal conduct that strain the conceptual foundations of contemporary criminal law. This research examines the phenomenon of AI-enabled crimes in India and evaluates the capacity of the country's reformed criminal justice framework, particularly the Bharatiya Nyaya Sanhita, 2023 (BNS), the Information Technology (IT) Act, 2000, and allied regulatory instruments, to address such emerging harms. It argues that despite the replacement of the colonial-era Indian Penal Code (IPC), 1860 with the BNS, India's penal framework continues to rely on anthropocentric assumptions of intent, causation, and agency, rendering it ill-suited to crimes characterized by algorithmic autonomy, opacity, scalability, and distributed responsibility. The research delves into core criminal law doctrines, such as *mens rea*, attribution of liability, evidentiary standards, and corporate culpability in the context of AI-mediated conduct, exposing persistent doctrinal and enforcement gaps. It further critiques India's fragmented and predominantly soft-law approach to AI governance, marked by sector-specific guidelines and ethical frameworks lacking binding force, and situates this within a comparative analysis of emerging international regulatory models. The research contends that the absence of a comprehensive statutory framework for AI accountability risks regulatory paralysis, either by under-criminalizing serious algorithmic harms or by adopting overbroad penal responses that may stifle innovation. It concludes by advocating a recalibrated, risk-sensitive, and anticipatory legal framework capable of harmonizing technological progress with the imperatives of legality, accountability, and constitutional governance.

Keywords: Artificial Intelligence, Criminal Liability, Algorithmic Accountability, Mens Rea, Cybercrime, Deepfakes, Autonomous Systems

BACKGROUND

The most recent governmental report addressing the intersection of AI innovation, crimes, and India's regulatory framework is the India AI Governance Guidelines, released by the Ministry of Electronics and Information Technology (MeitY) on November 05, 2025. This comprehensive framework, developed by a committee formed in July, 2025, builds on a January 2025 draft that received over 2,500 public submissions. It emphasizes balancing AI's transformative potential with safeguards against illegality, without introducing a standalone AI law at this stage. Instead, it advocates for agile, pro-innovation regulation through existing laws, voluntary measures, and future amendments. The guidelines highlight AI's risks, including criminal misuse, while promoting "innovation over restraint" to foster India's AI ecosystem Government of India, Ministry of Electronics and Information Technology (2025).

Key themes include human-centric AI design, fairness, accountability, and resilience. The report positions India as a global leader in responsible AI, drawing from international standards (such as ISO/ IEC) and domestic initiatives, such as India AI Mission, which aims to democratize AI access.

The guidelines identify AI as a double-edged sword, enabling innovation in sectors like healthcare, agriculture, and finance, but also facilitating crimes that exploit its autonomy and scalability. Malicious uses include (LexOrbis, 2026):

- *Deepfakes and Synthetic Content:* AI-generated audio/video for impersonation, identity theft, forgery, defamation, and spreading misinformation. This can incite public mischief or target vulnerable groups, such as women (e.g., non-consensual intimate images or "revenge porn") and children (such as - AI-generated child sexual abuse material, CSAM).
- *Cybercrimes and Attacks:* AI-driven trojan attacks, model/data poisoning, adversarial inputs disrupting critical infrastructure, and automated fraud like money laundering or phishing at scale.
- *National Security Threats:* AI-enabled cyberattacks on power grids, transportation, or defense systems; lethal autonomous weapons; and hybrid threats combining disinformation with physical harm.
- *Bias and Discrimination:* Algorithmic biases leading to unfair outcomes in hiring, lending, or policing, exacerbating social exclusion for marginalized communities.
- *Other Harms:* Loss of control over autonomous AI agents, environmental unsustainability from resource-intensive models, and systemic risks like market concentration or geopolitical disruptions in the AI supply chain.

The report defines “AI incidents” as events causing harm, such as physical injury, human rights violations, or environmental damage from AI malfunctions. While specific crime statistics are limited, it references broader trends, for instance, deepfakes accounted for 40% of biometric fraud globally in 2024 (cited from external reports like the Identity Fraud Report 2025), with predictions of increased malicious use in India per the India Cyber Security Threat Report 2025. Domestically, the guidelines note rising AI-facilitated harms, including over 90% of global deepfakes targeting women, as reported by the National Cyber Crime Reporting Portal in 2025, as delineated under Figure 1 hereinbelow (Srikant, M. (2025).

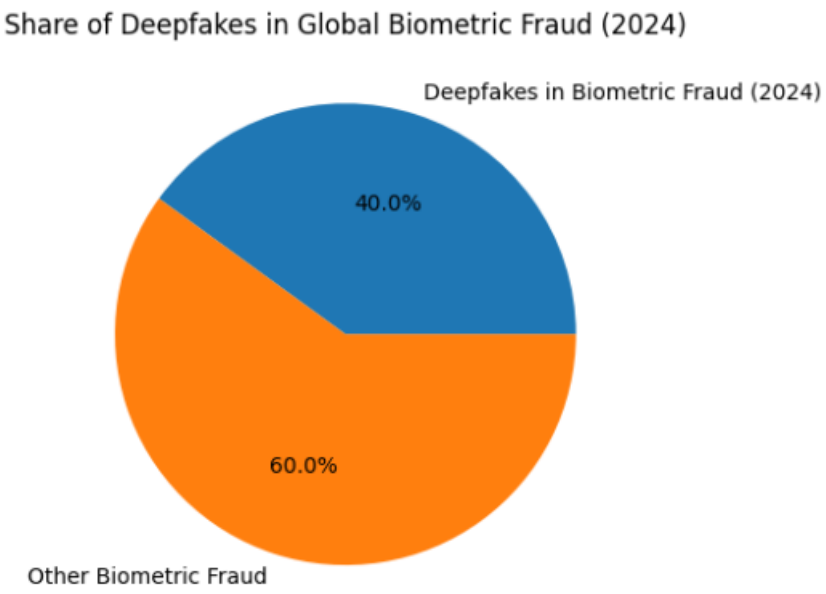

Figure 1

As of August, 2025, over 38,231 subsidized GPUs are available for startups and researchers, with a secure cluster of 3,000 next-gen GPUs for strategic use. The AIKosh platform hosts 1,500 datasets and 217 AI models from 34 entities across 20 sectors, while the India AI Application Development Initiative (IADI) has 30 sectoral prototypes underway. Capacity-building efforts support over 500 PhD fellows, 8,000 undergraduates, and 5,000 postgraduates in AI programs as delineated under Figure 2 hereinbelow (National e-Governance Division (2025).

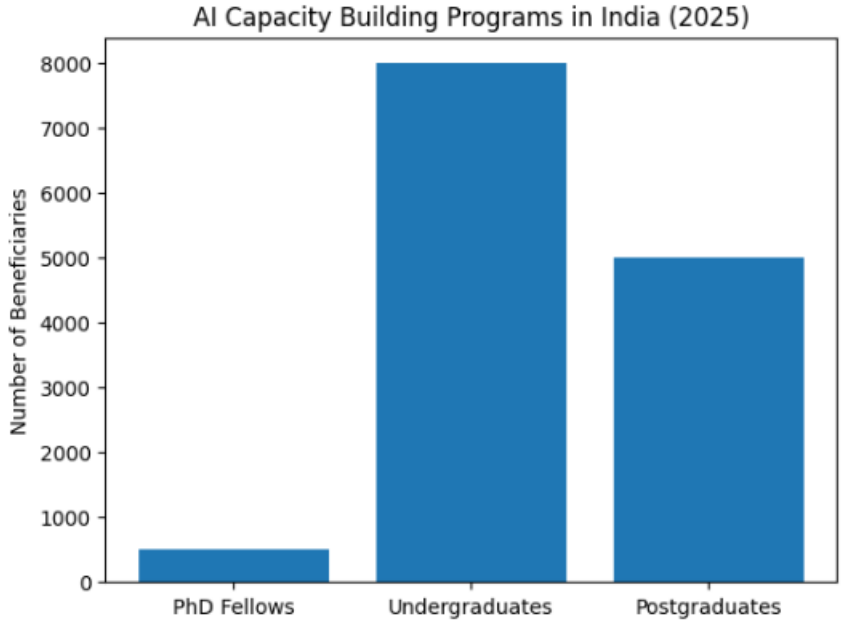

Figure 2

STATEMENT OF PROBLEM

The rapid proliferation of AI technologies has fundamentally disrupted traditional notions of criminal culpability and regulatory control within the Indian legal system. Existing penal doctrines, rooted in anthropocentric assumptions of intent, agency, and causation, are ill-equipped to address harms arising from autonomous or algorithm-driven conduct. The absence of AI-specific criminal standards and a fragmented regulatory framework have resulted in uncertainty in liability attribution, enforcement inefficiencies, and normative gaps that threaten both legal accountability and public trust.

RESEARCH QUESTIONS

- What constitutes an AI-enabled or AI-facilitated crime, and how should such conduct be distinguished from conventional technology-assisted offenses within criminal law?
- To what extent are India's existing penal and regulatory frameworks capable of addressing the unique harms and accountability challenges posed by AI systems?
- Where do doctrinal, institutional, and enforcement gaps exist in attributing liability and ensuring accountability for AI-related criminal conduct in India?

RESEARCH OBJECTIVES

- To critically examine the nature and scope of AI-enabled criminal conduct within the Indian legal and socio-technological context.
- To assess the adequacy and limitations of existing Indian penal and regulatory laws in responding to crimes involving artificial intelligence.
- To propose coherent legal and regulatory reforms aimed at strengthening accountability while preserving technological innovation.

RESEARCH METHODOLOGY

The study adopts a doctrinal research methodology, involving a systematic analysis of statutory provisions, judicial precedents, regulatory instruments, and scholarly literature relevant to AI and criminal law. Primary sources such as legislation and case law are examined alongside secondary sources including academic commentary and policy reports to evaluate the doctrinal soundness and practical efficacy of India's existing legal framework. Comparative references are used selectively to contextualize and strengthen normative conclusions.

CONCEPTUAL FRAMEWORK: UNDERSTANDING ARTIFICIAL INTELLIGENCE AND AI CRIMES

AI, though not statutorily defined in Indian law, is generally understood as computational systems capable of performing tasks that ordinarily require human intelligence, including learning, reasoning, prediction, and decision-making. Most contemporary legal concerns relate to *Narrow AI*, systems designed for specific functions such as facial recognition, recommendation algorithms, or automated trading, rather than *Artificial General Intelligence*, which remains largely theoretical. Narrow AI systems are typically powered by machine learning and deep learning techniques that rely on large datasets and probabilistic models, often operating with limited human intervention and, in certain cases, functional autonomy. Indian courts have begun to encounter these technologies indirectly; for instance, in *Anuradha Bhasin v. Union of India (AIR 2020 SUPREME COURT 1308)*, court acknowledged the pervasive role of digital technologies and algorithms in governance and information control, implicitly recognizing the legal salience of automated decision-making systems.

AI-related crimes may be conceptually classified based on the role AI plays, first, as a tool, where AI merely enhances human criminal intent (as seen in AI-driven phishing, deepfake scams, or automated misinformation); second, as an accomplice, where algorithmic systems materially influence or determine outcomes, such as credit approvals or predictive policing; and third, as a semi-autonomous

actor, where harm results from AI systems operating with minimal real-time human control, raising difficult questions of attribution and mens rea. The distinctive features of AI crimes, unprecedented scale and speed, anonymity enabled by automated systems, cross-border data flows, & opacity of algorithmic decision-making, strain foundational criminal law doctrines. Courts have long relied on foreseeability and intent, yet the "black box" nature of deep learning systems undermines predictability and explainability, complicating the evidentiary burden & assessment of culpability, as highlighted by comparative judicial discourse and increasingly echoed in Indian regulatory debates.

TYPOLOGY OF AI-ENABLED CRIMINAL ACTIVITIES IN INDIA

In the Indian context, AI-enabled criminality has manifested most visibly in the domains of cyber and financial crimes, identity-related harms, surveillance abuses, algorithmic discrimination, and physical harms caused by autonomous systems. Law enforcement agencies have reported a surge in AI-driven phishing and social engineering attacks that mimic human speech and behavior with alarming sophistication, while algorithmic manipulation in securities trading poses systemic risks to market integrity, engaging concerns under SEBI regulations & broader anti-fraud framework. Deepfakes and synthetic media have emerged as potent tools for political misinformation and non-consensual sexual imagery, threatening electoral integrity, dignity, and privacy; although courts have not yet adjudicated extensively on deepfakes, jurisprudence on reputation and free speech, such as *Subramanian Swamy v. Union of India (WRIT PETITION (CRIMINAL) NO. 184 OF 2014)*, provides only partial guidance in addressing algorithmically amplified defamation.

Surveillance and privacy violations through facial recognition technologies and unauthorized data profiling raise constitutional concerns under Art. 21, especially after *Justice K.S. Puttaswamy (Retd.) & Anr. v. Union of India & Ors. (2019 (1) SCC 1)*, which affirmed informational privacy and decisional autonomy as fundamental rights. Further, algorithmic bias in hiring, policing, and credit scoring illustrates how AI can produce discriminatory outcomes as systemic harm, often without explicit intent, challenging equality norms under Art. 14 and 15. Further the deployment of AI in autonomous vehicles, drones, and medical or industrial systems introduces the risk of physical harm, where failures may stem from data bias, design flaws, or unforeseen system behavior. Indian tort and criminal law remain ill-equipped to address such harms, as existing frameworks presuppose human agency and direct causation.

EXISTING PENAL FRAMEWORK IN INDIA: APPLICABILITY AND LIMITATIONS

The guidelines affirm that no dedicated AI law is currently needed, as existing statutes can address many issues, though with adaptations. Key elements include:

- *Criminal Laws:* BNS, 2023, penalizes AI-enabled offenses like cheating by personation (Sec. 319), forgery (Sec. 336), obscene material distribution (Sec. 294, 296), defamation (Sec. 356), organized crime (Sec. 111), and public mischief (Sec. 353). The Prevention of Children from Sexual Offences Act, 2012, covers AI-generated CSAM.

- *IT and Data Protection Laws:* The Information Technology (IT) Act, 2000 (amended 2008), handles cybercrimes via Sec. 66D (impersonation), 66E (privacy violation), 67 (obscene content), and 79 (intermediary liability with due diligence requirements). The Digital Personal Data Protection Act (DPDPA), 2023, mandates consent, data minimization, and purpose limitation for AI training, with fines up to ₹250 crore for breaches. The Bharatiya Sakshya Adhiniyam, 2023, requires authentication for electronic evidence like deepfakes (Sec. 63).

- *Consumer and Sectoral Regulations:* The Consumer Protection Act, 2019, targets misleading AI claims or dark patterns. Sector-specific rules include RBI's Framework for Responsible, Explainable, and Ethical AI (FREE-AI) Report (2025) for banking (Reserve Bank of India, 2025), SEBI's guidelines on AI in securities (June, 2025), IRDAI's cyber security mandates for insurers, and ICMR's ethical guidelines for AI in healthcare. CERT-In Directions (2022) require 6-hour incident reporting for cybersecurity breaches in AI systems.

- *Other Protections:* Copyright Act, 1957 (Sec. 52 delineates limited exemptions for AI training); Rights of Persons with Disabilities Act, 2016; and Telecommunications Act, 2023, for infrastructure security.

These laws emphasize *mens rea* (guilty intent) for humans behind AI, with vicarious liability for developers, deployers, or users.

REGULATORY LANDSCAPE GOVERNING ARTIFICIAL INTELLIGENCE IN INDIA

In the Indian legal order, the regulatory landscape governing AI remains a patchwork of generalist statutes, sectoral edicts, and aspirational policy documents rather than a cohesive framework capable of grappling with AI's unique risks. The DPDPA, 2023 (born of the *Puttaswamy*'s privacy doctrine) establishes a foundational right to data protection and imposes obligations on data fiduciaries for fair processing and consent-based data handling, but it is technology neutral and conspicuously silent on crucial AI fingerprints such as algorithmic profiling, automated decision-making transparency, explainability, bias mitigation, and meaningful contestability of automated outcomes, leaving an accountability void in contexts where opaque models shape credit scores, employment decisions, or public service entitlements (Krishna, G. (2022).

Sector-specific regulation, such as RBI's guidelines on the governance of AI in fintech, mandating fairness, auditability, and risk governance for algorithmic models, and SEBI's directives on the use of AI/ ML in trading and advisory services, provide domain-bound controls but are inherently limited in scope and enforcement reach, failing to articulate statutory sanctions or uniform standards applicable across domains. Parallel soft-law instruments, notably NITI Aayog's "National Strategy for Artificial Intelligence (#AIforAll)" and related ethical AI principles, articulate non-binding values, such as transparency, safety, non-discrimination, and accountability; while important for norm-setting, they lack legal enforceability and thus cannot, in themselves, generate remedies or compliance obligations in judicial proceedings (Kayara Legal (2025).

The absence of a dedicated, horizontal AI statute results in regulatory fragmentation, with responsibilities diffused across MeitY, RBI, SEBI, and other bodies, creating interpretive uncertainty and compliance lacunae; this over-reliance on generalist laws and sectoral rules undermines doctrinal clarity on liability and fails to address algorithmic risk profiles in a manner commensurate with India's constitutional commitments to equality, privacy, and due process (Drishti IAS, 2025).

CRIMINAL LIABILITY AND ACCOUNTABILITY IN AI CRIMES

In the domain of criminal liability and accountability for AI-enabled harms, the Indian legal framework remains largely anthropocentric, grounded in traditional constructs of culpability that presuppose human agency & mens rea, making attribution of responsibility to developers, deployers, users, and data providers legally fraught when harms emerge from complex autonomous systems. Contemporary jurisprudence illustrates this tension, while courts have not yet articulated AI-specific criminal doctrines, they have applied existing statutes to AI harms, for example, deepfake creators being booked under IPC/ BNS for defamation and misuse of technology, as seen in recent FIRs and interim reliefs directed at content platforms for AI-generated misrepresentations that injure reputation and dignity (reflecting *Subramanian Swamy v. Union of India (WRIT PETITION (CRIMINAL) NO. 184 OF 2014)* affirmation of personality and reputation protection and Puttaswamy's constitutional privacy framework).

Consequently, there is a compelling case for strict liability in high-risk AI applications, akin to hazardous activity jurisprudence, where the deployment of an autonomous system creates inherently dangerous risks (such as algorithmic discrimination in credit or safety-critical decisioning), liability should attach irrespective of traditional *mens rea* to incentivize robust oversight and risk mitigation, aligning with comparative reforms that reframe duty of care in algorithmic governance (Tech Law Forum NALSAR, 2020).

Similarly, vicarious and product liability models, distinguishing AI as a product versus AI as a service, invite consumer protection principles that hold manufacturers and service providers accountable for defects and deficiencies, yet these are limited when AI systems self-learn beyond initial parameters and escape conventional defect definitions. This doctrinal inadequacy underscores the need for a new liability paradigm, algorithmic accountability frameworks and risk-based liability models that integrate statutory mandates for transparency, continuous auditing, and human-in-the-loop safeguards, ensuring that culpability does not evaporate in the "black box" of autonomous computation but is instead anchored in a regulatory design that balances innovation with enforceable standards of responsibility (Reddy, G. (2025).

COMPARATIVE AND INTERNATIONAL PERSPECTIVES

In the comparative and international dimension, the EU's AI Act represents a watershed in legal regulation by enshrining a risk-based regulatory architecture that stratifies AI systems into categories of unacceptable, high, limited, or minimal risk, imposes stringent compliance duties (such as risk mitigation, human oversight, quality data governance, transparency, and incident reporting) on high-impact systems, and empowers enforcement authorities with significant sanctions, fines of up to €35 million or 7% of global turnover for non-compliance, thereby operationalizing accountability in ways that resonate beyond the EU's borders by setting de facto global standards for AI risk governance (Mukherjee, S., & Meijer, B. H. (2025).

By contrast, the US lacks a comprehensive federal AI statute and instead relies on sector-specific regulatory regimes, existing criminal laws, and evolving prosecutorial guidance; for instance, the US Department of Justice has updated its Evaluation of Corporate Compliance Programs to integrate AI risk assessment and has signaled interest in AI-related sentencing enhancements where misuse "significantly contributed" to criminal conduct, while federal agencies like the FTC and SEC deploy consumer and securities laws to police deceptive AI practices, epitomizing a decentralized, innovation-oriented framework that emphasizes tort-based remedies and agency enforcement rather than ex ante AI governance (Government of the United Kingdom, 2023).

In UK, regulators have adopted a principles-based, sector-led approach anchored in the National AI Strategy and AI White Paper that refrains from broad horizontals, instead tasking existing sector regulators to adapt common law doctrines such as negligence and breach of statutory duty to algorithmic harms, and retaining flexibility to evolve through both statutory initiatives (such as proposed AI authority concepts) and sectoral data and safety legislation rather than a single, comprehensive AI statute (Kumar, M. (2025).

For India, these contrasting models offer critical lessons, harmonizing innovation with safeguards demands proportionate, risk-based regulation that avoids both regulatory voids and over-criminalization, drawing on the EU's structured categorization of risk and compliance obligations while preserving the innovation-friendly, adaptable enforcement ethos exemplified in US and UK sectoral approaches; such calibrated synthesis is essential for a legal regime capable of responding to AI's multifaceted harms without stifling technological progress.

ENFORCEMENT CHALLENGES AND INSTITUTIONAL CONSTRAINTS

In the Indian context, the enforcement architecture for AI-enabled and cyber-enabled crimes reveals profound structural constraints that blunt the rule of law and impede credible deterrence, law enforcement agencies and investigative wings, whether at the Cyber Crime Coordination Centre (I4C) or state cyber cells, lack the specialized technical capacity and AI forensics expertise necessary to detect, trace, and attribute algorithmic harms, a gap repeatedly noted in legal scholarship on India's cybercrime readiness and forensic deficits. Courts have implicitly acknowledged this lacuna by mandating institutional strengthening, as the Hon'ble Karnataka High Court recently underscored the need for a robust cyber command centre to effectively grapple with the surge in cyber offences, yet such pronouncements highlight reactive adjudication rather than proactive capability building. The practical consequence is a growing dependence on private forensic experts and external technical consultants, which in turn raises concerns about evidentiary reliability, chain of custody, and impartiality in prosecutions (Kumar, P. V. (2025).

Jurisdictionally, Indian law's traditional territorial principles have been strained by the borderless nature of digital and AI-facilitated wrongdoing, leaving courts and investigators grappling with extraterritorial application & slow, bureaucratic mechanics of Mutual Legal Assistance Treaties (MLATs) for evidence sharing and extradition, which are ill-suited to the near-real-time exigencies of AI crimes. India's continued non-adherence to the Budapest Convention further isolates its enforcement regime from harmonized international protocols for cybercrime cooperation, exacerbating delays and legal uncertainty. Compounding these transnational hurdles is domestic regulatory fragmentation, overlapping provisions in the IT Act, BNS/ IPC, and emerging statutory instruments produce ambiguity over prosecutorial mandates and investigative jurisdiction, with courts such as the Hon'ble Orissa High Court even clarifying the concurrent investigative powers of local police stations in cyber offences, an acknowledgment of the systemic fuzziness plaguing enforcement structures (The Times of India, 2025).

CONCLUSION & A WAY FORWARD

The uneasy coexistence of artificial intelligence-driven innovation & reality of criminal misuse exposes the structural inadequacy of India's existing penal and regulatory framework, which remains rooted in anthropocentric assumptions of intent, control, and foreseeability that AI systems fundamentally disrupt. The present reliance on IPC/ BNS, IT Act, and fragmented sectoral regulations results in doctrinal uncertainty, enforcement paralysis, and accountability deficits, particularly in cases involving autonomous or opaque algorithmic decision-making. A coherent way forward demands a shift from reactive, offence-specific criminalization to a principled, risk-based regulatory architecture that integrates criminal liability with ex ante governance mechanisms. This must include statutory recognition of algorithmic accountability, calibrated standards of negligence and strict liability for high-risk AI deployments, mandatory auditability & explainability obligations, & institutional capacity-building for law enforcement & judiciary. Crucially, reform must avoid innovation-chilling overreach by embedding proportionality, regulatory sandboxes, and human-in-the-loop safeguards, thereby ensuring that technological progress is harmonized with constitutional values, due process, & imperatives of the rule of law.

REFERENCES

- Government of India, Ministry of Electronics and Information Technology. (2025). *India AI governance guidelines: Enabling safe and trusted AI innovation* [Report]. IndiaAI Mission. https://indiaai.s3.ap-south-1.amazonaws.com/docs/guidelines-governance.pdf.
- LexOrbis. (2026, January 13). *Moving towards responsible and ethical use of AI: Analysis of India's proposed AI Bill, 2025*. https://www.lexorbis.com/moving-towards-responsible-and-ethical-use-of-ai-analysis-of-indias-proposed-ai-bill-2025/.
- Srikant, M. (2025, April 28). *Bharatiya laws against deepfake cybercrime: Opportunities and challenges*. Vivekananda International Foundation. https://www.vifindia.org/article/2025/april/28/Bharatiya-Laws-Against-Deepfake-Cybercrime-Opportunities-and-Challenges.
- National e-Governance Division. (2025, September 29). *Deepfakes in India: Legal landscape, judicial responses, and a practical playbook for enforcement*. https://negd.gov.in/blog/deepfakes-in-india-legal-landscape-judicial-responses-and-a-practical-playbook-for-enforcement/.
- Reserve Bank of India. (2025, August). *FREE-AI Committee report*. https://rbidocs.rbi.org.in/rdocs/PublicationReport/Pdfs/FREEAIR130820250A2 4FF2D4578453F824C72ED9F5D5851.PDF.

- Krishna, G. (2022). *AI regulation in India: Bridging legislative gaps through global governance standards*. *International Journal of Legal Studies and Social Sciences*, *3*(6), 28–34.
- *Kayara Legal*. (2025, June 6). *AI and machine learning in fintech: Navigating ethical and regulatory risks*. https://www.kayaralegal.com/2025/06/06/ai-and-machine-learning-in-fintech-navigating-ethical-and-regulatory-risks/.
- Drishti IAS. (2025, December 31). *Shaping responsible AI: India's evolving regulatory framework*. Drishti IAS. https://www.drishtiias.com/daily-updates/daily-news-editorials/shaping-responsible-ai-indias-evolving-regulatory-framework.
- Tech Law Forum NALSAR. (2020, December 24). *Principled artificial intelligence: Adopting the principle of AI accountability and responsibility in India*. https://techlawforum.nalsar.ac.in/principled-artificial-intelligence-adopting-the-principle-of-ai-accountability-and-responsibility-in-india/.
- Reddy, G. (2025). Suit against artificial intelligence: Consequences – A critical analysis. *International Journal of Academic Research*, 12(3).
- Mukherjee, S., & Meijer, B. H. (2025, November 19). *EU to delay 'high risk' AI rules until 2027 after Big Tech pushback*. Reuters. https://www.reuters.com/sustainability/boards-policy-regulation/eu-delay-high-risk-ai-rules-until-2027-after-big-tech-pushback-2025-11-19/#:~:text='HIGH%20RISK'%20AI%20USE%20IN%20JOB%20APPLICATIONS%2C%20BIOMETRICS&text=In%20a%20'Digital%20Omnibus'%2C,December%202027%20from%20August%202026.
- Government of the United Kingdom. (2023, August 3). *A pro-innovation approach to AI regulation* [Policy paper]. https://www.gov.uk/government/publications/ai-regulation-a-pro-innovation-approach/white-paper.
- Kumar, M. (2025, August 28). *Explainer: AI and criminal liability – A global and Indian legal perspective*. Neuro Amicus. https://news.neuroamicus.com/ai-criminal-liability-global-indian-legal-perspective/.
- Kumar, P. V. (2025, September 11). *Strong cyber command centre is a necessity now: Karnataka high court*. *The Times of India*. https://timesofindia.indiatimes.com/city/bengaluru/strong-cyber-command-centre-is-a-necessity-now-karnataka-high-court/articleshow/123815737.cms.
- The Times of India. (2025, August 26). *HC: Local police stations have power to investigate cyber offences.* https://timesofindia.indiatimes.com/city/bhubaneswar/hc-local-police-stations-have-power-to-investigate-cyber-offences/articleshow/123510607.cms.