KNOWLEDGE FLAME
E-ISSN: 3049-1541
International Multidisciplinary Research Journal (KF-IMRJ)
(An International Indexed & Peer Reviewed Journal
Impact Factor: 5.292 https://knowledgeflame.in PRGI Reg. No. MAHMUL/2024/89852

Artificial Intelligence in India: Accountability, Misuse and Legal Protection

Mr Satish K Gujar
Research Scholar
Arts, Science and Commerce College, Ambad Dist. Jalna – 431209
gujarambad@gmail.com

Dr Shivaji K Taur
Assistant Professor, Dept. of Economics
Arts, Science and Commerce College, Ambad Dist. Jalna – 431209
tsrajeshivaji05@gmail.com

Introduction:

Artificial Intelligence (AI) is reshaping multiple sectors in India — from healthcare and finance to law enforcement and governance. This research article provides a detailed examination of the legal dimensions of AI in India, focusing on accountability, avenues of misuse, and existing and proposed legal protections. It synthesizes policy context, current legal instruments, gaps, recommendations, and practical steps for regulators and organizations.

Executive Summary

India currently relies on a patchwork of sectoral statutes and policy documents (DPDPA, IT Act, sectoral guidelines, NITI Aayog reports, and MeitY consultations) to regulate AI- related harms. Accountability remains ambiguous for many AI deployments, while misuse such as deepfakes, AI-driven fraud, and mass surveillance is growing. This paper recommends a risk-based AI law, clearer liability allocation, mandatory audits for high- risk systems, and targeted measures against deepfakes and automated fraud.

Detailed Legal Landscape in India

The following table summarises principal laws, policies, and their relevance to AI in India:

Law/Policy	Relevance to AI	Limitations
Digital Personal Data Protection Act, 2023 (DPDPA)	Governs digital personal data processing; consent, obligations	Does not directly regulate algorithms or automated decision-making
Information Technology Act, 2000 (IT Act)	Cybersecurity, intermediary liability, electronic records	Outdated for many AI-specific harms (deepfakes, generative AI)
Consumer Protection Act, 2019	Liability for defective goods/services (including AI-enabled products)	No clarity on responsibility between developer and deployer
Sectoral Guidelines (RBI, SEBI, MoHFW, IRDAI)	Sector-specific oversight: fintech, healthcare, insurance, securities	Fragmented; inconsistent across sectors
Proposed Digital India Act (DIA)	Expected to modernize IT Act, include content moderation and new governance	Drafting stage; details and timelines uncertain

Key reference points:

- Digital Personal Data Protection Act, 2023: establishes data processing obligations and significant data fiduciary provisions.
- Information Technology Act, 2000: remains India's primary cyber statute but is dated for modern AI harms.

KNOWLEDGE FLAME
E-ISSN: 3049-1541
International Multidisciplinary Research Journal (KF-IMRJ)
(An International Indexed & Peer Reviewed Journal
Impact Factor: 5.292 https://knowledgeflame.in PRGI Reg. No. MAHMUL/2024/89852

- NITI Aayog's AI strategy and MeitY's ongoing AI governance consultations are shaping policy direction.

Accountability: Who is Responsible?

Assigning accountability for AI-related harms involves legal, technical, and organizational considerations. The table below maps typical use-cases, harms, accountable parties, and legal gaps:

Use Case	Potential Harm	Potential Accountable Parties	Legal Gaps
Autonomous Vehicles	Accidents causing injury/death	Manufacturer, software developer, fleet operator	No precedent; requires product liability clarity
AI in Banking & Lending	Algorithmic bias; wrongful denial of service/credit	Bank/Platform, model vendor, data provider	No mandatory fairness audits; weak disclosure norms
Facial Recognition in Policing	Wrongful identification; privacy breach	Law enforcement agency, vendor	Weak oversight and transparency; constitutional concerns
Healthcare AI	Misdiagnosis; patient harm	Hospital/clinician, AI developer	Regulation patchy; clinical validation standards needed

Discussion:

In many scenarios Indian courts would apply existing negligence, contract, or product liability doctrines. However, AI introduces opacity (black-box models), continuous learning, and multi-party supply chains (data providers, model developers, deployers), complicating fault allocation. Policy options include: mandatory risk assessments, strict liability for certain autonomous harms, and clarity in service-vendor contracts.

Misuse of AI: Forms, Examples, and Legal Status

The following table summarises common misuse categories, examples, and their current legal status in India:

Form of Misuse, Examples/Consequences, Current Legal Status Deepfakes and Politically-motivated Manipulation, "Election-time misinformation, defamation, harassment", No specific statute for deepfakes; IPC/IT Act used indirectly "Automated Financial Fraud (voice-cloning, phishing)",Significant monetary loss to victims and institutions, Covered under IT Act/IPC but enforcement challenging Mass Surveillance & Facial Recognition, "Erosion of privacy, chilling effect on civil liberties", Raises right to privacy issues (Puttaswamy Judgment) Algorithmic Bias & Discrimination, "Marginalization in hiring, credit, policing", No statutory fairness or audit obligations Misinformation Amplification (automated bots),"Social unrest, reputational harm", Content moderation rules exist but enforcement and detection remain weak

KNOWLEDGE FLAME
E-ISSN: 3049-1541
International Multidisciplinary Research Journal (KF-IMRJ)
(An International Indexed & Peer Reviewed Journal
Impact Factor: 5.292 https://knowledgeflame.in PRGI Reg. No. MAHMUL/2024/89852

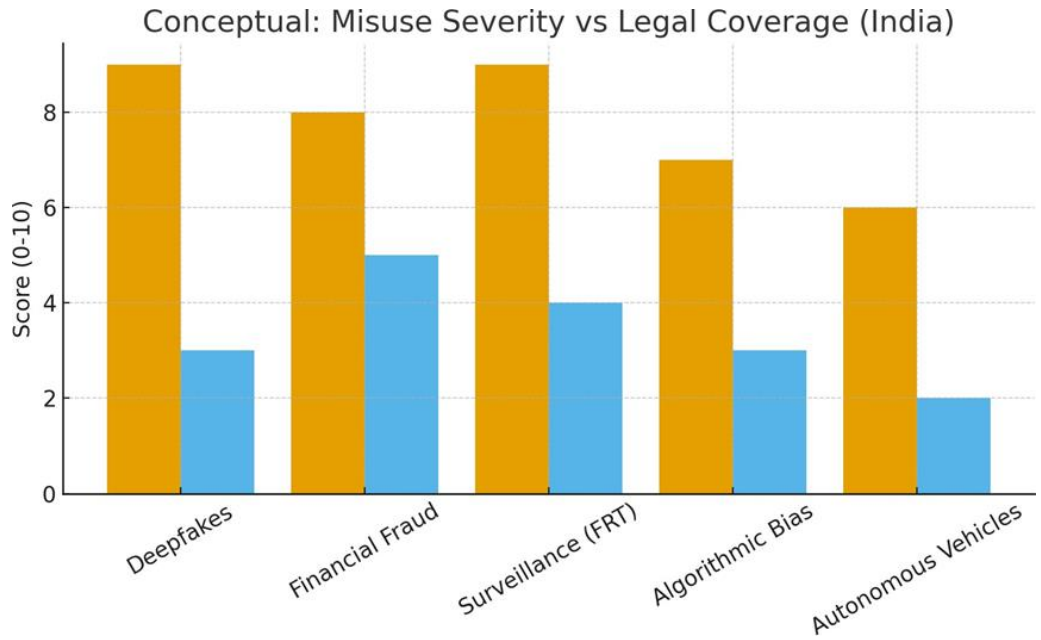
Form of Misuse	Examples/Consequences	Current Legal Status
Deepfakes and Politically-motivated Manipulation	Election-time misinformation, defamation, harassment	No specific statute for deepfakes; IPC/IT Act used indirectly
Automated Financial Fraud (voice-cloning, phishing)	Significant monetary loss to victims and institutions	Covered under IT Act/IPC but enforcement challenging
Mass Surveillance & Facial Recognition	Erosion of privacy, chilling effect on civil liberties	Raises right to privacy issues (Puttaswamy judgment)
Algorithmic Bias & Discrimination	Marginalization in hiring, credit, policing	No statutory fairness or audit obligations
Misinformation Amplification (automated bots)	Social unrest, reputational harm	Content moderation rules exist but enforcement and detection remain weak

Notable recent developments (examples):

- CERT-In advisories and government advisories on deepfake threats and countermeasures.
- Parliamentary recommendations urging tougher rules on deepfakes, OTT platforms and social media.

5. Chart: Misuse Severity vs Legal Coverage (Conceptual)

The chart below is conceptual—intended to illustrate where high-severity misuse converges with low legal coverage in India. (High score = greater severity / stronger legal coverage).



Legal Protections: Existing Remedies and Their Limits:

Existing legal instruments (DPDPA, IT Act, IPC, Consumer Protection Act, and sectoral circulars) provide remedies for data breaches, cybercrime, fraud, and consumer harms. However, these laws are often applied indirectly to AI harms, leading to uncertainty. Key

KNOWLEDGE FLAME
E-ISSN: 3049-1541
International Multidisciplinary Research Journal (KF-IMRJ)
(An International Indexed & Peer Reviewed Journal
Impact Factor: 5.292 https://knowledgeflame.in PRGI Reg. No. MAHMUL/2024/89852

limitations include absence of AI- specific regulation, lack of mandatory fairness or safety audits, limited transparency obligations, and enforcement capacity constraints.

Recommendations for Lawmakers and Practitioners:

- Enact a risk-based AI framework (e.g., Digital India Act + AI rules) that categorizes systems by risk and prescribes corresponding obligations.
- Clarify liability: define roles and responsibilities for data providers, model developers, deployers, and operators. Consider strict liability for certain autonomous harms.
- Mandate AI impact assessments and independent audits for high-risk systems (health, finance, policing).
- Criminalize malicious deepfake creation and distribution where used for fraud, extortion, or election interference; ensure proportionality and due process.
- Strengthen data governance: transparency obligations, provenance logging, and rights to explanation for automated adverse decisions.
- Build technical and enforcement capacity (CERT-In, police cyber cells, regulators) with guidelines for detection and rapid response to AI misuse.
- Promote public–private collaboration for dataset stewardship, open standards for provenance, and shared red-teaming resources.
- Implementation Roadmap (Practical Steps)
- Short term (6-12 months): Issue targeted advisories (deepfakes, financial fraud), require high-risk registries, and publish model documentation guidance.
- Medium term (1-3 years): Pass risk-based AI rules, implement mandatory audits for critical sectors, and operationalize DPDPA enforcement mechanisms.
- Long term (3-5 years): Create statutory frameworks for liability apportionment, invest in AI-labelling/provenance infrastructure, and harmonize with global standards.

Appendix: Tables (CSV-friendly) & Sources

The tables used in this document are included in CSV-friendly form at the end of this Word document for reuse.

Legal Landscape (CSV):

Law/Policy, Relevance to AI, Limitations "Digital Personal Data Protection Act, 2023 (DPDPA)","Governs digital personal data processing; consent, obligations", Does not directly regulate algorithms or automated decision-making "Information Technology Act, 2000 (IT Act)","Cybersecurity, intermediary liability, electronic records", "Outdated for many AI-specific harms (deepfakes, generative AI)" "Consumer Protection Act, 2019",Liability for defective goods/services (including AI-enabled products),No clarity on responsibility between developer and deployer "Sectoral Guidelines (RBI, SEBI, MoHFW, IRDAI)","Sector-specific oversight: fintech, healthcare, insurance, securities", Fragmented; inconsistent across sectors Proposed Digital India Act (DIA),"Expected to modernize IT Act, include content moderation and new governance", Drafting stage; details and timelines uncertain.

KNOWLEDGE FLAME
E-ISSN: 3049-1541
International Multidisciplinary Research Journal (KF-IMRJ)
(An International Indexed & Peer Reviewed Journal
Impact Factor: 5.292 https://knowledgeflame.in PRGI Reg. No. MAHMUL/2024/89852

Accountability:

Use Case, Potential Harm, Potential Accountable Parties, Legal Gaps Autonomous Vehicles, Accidents causing injury/death, "Manufacturer, software developer, fleet operator", No precedent; requires product liability clarity AI in Banking & Lending,Algorithmic bias; wrongful denial of service/credit, "Bank/Platform, model vendor, data provider", No mandatory fairness audits; weak disclosure norms Facial Recognition in Policing, Wrongful identification; privacy breach, "Law enforcement agency, vendor", Weak oversight and transparency; constitutional concerns Healthcare AI, Misdiagnosis; patient harm, "Hospital/clinician, AI developer", Regulation patchy; clinical validation standards needed

Conclusion:

India stands at a crossroads: AI offers transformative benefits but also raises urgent legal and social questions about accountability and misuse. A balanced legal approach combining risk-based regulation, clearer liability rules, technical preparedness, and targeted criminal measures is essential to protect rights while enabling innovation.

References:

1. Digital Personal Data Protection Act, 2023 (official text). MeitY
2. NITI Aayog — National Strategy for Artificial Intelligence / Responsible AI principles. NITI Aayog+1
3. Supreme Court — Puttaswamy v. Union of India (Right to Privacy, 2017). Human Dignity TrustSupreme Court Observer
4. MeitY report on AI governance guidelines and public consultation. IndiaAI
5. Recent government/Parliament activity and advisories on deepfakes & online harms (CERT-In advisory; Parliamentary recommendations).