INTERNATIONAL JOURNAL FOR LEGAL RESEARCH AND ANALYSIS

Open Access, Refereed Journal Multi Disciplinary
Peer Reviewed

www.ijlra.com

ISSN: 2582-6433

DISCLAIMER

No part of this publication may be reproduced, stored, transmitted, or distributed in any form or by any means, whether electronic, mechanical, photocopying, recording, or otherwise, without prior written permission of the Managing Editor of the *International Journal for Legal Research & Analysis (IJLRA)*.

The views, opinions, interpretations, and conclusions expressed in the articles published in this journal are solely those of the respective authors. They do not necessarily reflect the views of the Editorial Board, Editors, Reviewers, Advisors, or the Publisher of IJLRA.

Although every reasonable effort has been made to ensure the accuracy, authenticity, and proper citation of the content published in this journal, neither the Editorial Board nor IJLRA shall be held liable or responsible, in any manner whatsoever, for any loss, damage, or consequence arising from the use, reliance upon, or interpretation of the information contained in this publication.

The content published herein is intended solely for academic and informational purposes and shall not be construed as legal advice or professional opinion.

ISSN: 2582-6433

ABOUT US

The *International Journal for Legal Research & Analysis (IJLRA)* (ISSN: 2582-6433) is a peer-reviewed, academic, online journal published on a monthly basis. The journal aims to provide a comprehensive and interactive platform for the publication of original and high-quality legal research.

IJLRA publishes Short Articles, Long Articles, Research Papers, Case Comments, Book Reviews, Essays, and interdisciplinary studies in the field of law and allied disciplines. The journal seeks to promote critical analysis and informed discourse on contemporary legal, social, and policy issues.

The primary objective of IJLRA is to enhance academic engagement and scholarly dialogue among law students, researchers, academicians, legal professionals, and members of the Bar and Bench. The journal endeavours to establish itself as a credible and widely cited academic publication through the publication of original, well-researched, and analytically sound contributions.

IJLRA welcomes submissions from all branches of law, provided the work is original, unpublished, and submitted in accordance with the prescribed submission guidelines. All manuscripts are subject to a rigorous peer-review process to ensure academic quality, originality, and relevance.

Through its publications, the *International Journal for Legal Research & Analysis* aspires to contribute meaningfully to legal scholarship and the development of law as an instrument of justice and social progress.

ISSN: 2582-6433

PUBLICATION ETHICS, COPYRIGHT & AUTHOR RESPONSIBILITY STATEMENT

The *International Journal for Legal Research and Analysis (IJLRA)* is committed to upholding the highest standards of publication ethics and academic integrity. All manuscripts submitted to the journal must be original, unpublished, and free from plagiarism, data fabrication, falsification, or any form of unethical research or publication practice. Authors are solely responsible for the accuracy, originality, legality, and ethical compliance of their work and must ensure that all sources are properly cited and that necessary permissions for any third-party copyrighted material have been duly obtained prior to submission. Copyright in all published articles vests with IJLRA, unless otherwise expressly stated, and authors grant the journal the irrevocable right to publish, reproduce, distribute, and archive their work in print and electronic formats. The views and opinions expressed in the articles are those of the authors alone and do not reflect the views of the Editors, Editorial Board, Reviewers, or Publisher. IJLRA shall not be liable for any loss, damage, claim, or legal consequence arising from the use, reliance upon, or interpretation of the content published. By submitting a manuscript, the author(s) agree to fully indemnify and hold harmless the journal, its Editor-in-Chief, Editors, Editorial Board, Reviewers, Advisors, Publisher, and Management against any claims, liabilities, or legal proceedings arising out of plagiarism, copyright infringement, defamation, breach of confidentiality, or violation of third-party rights. The journal reserves the absolute right to reject, withdraw, retract, or remove any manuscript or published article in case of ethical or legal violations, without incurring any liability.

ISSN: 2582-6433

ASCRIBING LEGAL LIABILITY TO AGENTIC ARTIFICIAL INTELLIGENCE: RETHINKING INTENTION, CONTROL AND CAUSATION UNDER INDIAN LAW

AUTHORED BY – VASUMATHI.V
LL.M Final Year Student (Criminal Law) Crescent Law School,
B. S. Abdur Rahman Crescent Institute of Science & Technology, TN

ABSTRACT

The move from generative systems to agentic AI is a huge change in how humans and technology interact and evolve quickly. Traditional artificial intelligence systems mainly react to human instructions. Agent-based artificial intelligence systems, however, are increasingly able to plan tasks, make decisions, use digital resources, interface with external systems, and adapt their behaviour to achieve predefined goals with minimal human intervention. This advancement raises a basic legal question: when an AI agent acts freely and produces legal harm, who should be held liable? Indian law at now, is founded on ideas such as purpose, knowledge, control, negligence, causation and foreseeability. Indian law allocates criminal and civil liability to natural or juristic individuals in general. Agentic AI defies these established concepts as the immediate operational choice may not be directly made by its developer, user or deployer, but instead, created by a system.

This article critically analyses the adequacy of the Bharatiya Nyaya Sanhita, 2023, Information Technology Act, 2000, Bharatiya Sakshya Adhiniyam, 2023, Digital Personal Data Protection Act, 2023[1] and developing Indian AI-governance procedures to handle autonomous AI conduct. It examines key judicial principles on intermediary liability, privacy, electronic evidence, technology responsibility and corporate responsibility. The report recommends that AI should not be granted independent legal identity and suggests a human-centred accountability paradigm based on control, foreseeability, risk generation, benefit, monitoring and reasonable precautions. It calls for a statutory regime with required agent registration for high-risk uses, audit trails, human supervision, incident reporting, liability apportionment, technical standards and specialised regulatory agencies.

[1] Digital Personal Data Protection Act, No. 22 of 2023, §§ 4–8 (India).

ISSN: 2582-6433

INTRODUCTION

Artificial intelligence has gone beyond systems that simply create text, graphics, recommendations or forecasts. The direction in which present-day technology is moving is toward agentic artificial intelligence, where an AI system can be programmed to pursue a goal through a series of actions, using external tools, retrieving information, interacting with software applications and changing its approach in response to changing circumstances. Recent studies of Indian business show that enterprise adoption of AI is increasingly shifting toward more autonomous kinds of deployment. EY India's survey of more than 200 enterprise leaders finds that almost half of Indian organisations have multiple live generative-AI use cases, but just approximately 10 per cent have enterprise-wide deployment. The same report also cited data governance, security and integration as important difficulties. Industry reporting from 2026 suggests a strong desire among Indian companies to use agentic AI.

The importance of agentic AI is not just its technical sophistication, but the legal repercussions of delegating decision-making and execution to an artificial system. In a traditional software program, the program does what it is told to do, performing pre-defined functions. Agentic systems, in contrast, can choose intermediate stages, decide how a goal is to be reached, and communicate with other systems without a human approving each individual action.

This poses a fundamental challenge of legal attribution. Where an offence is intentionally committed by a human actor through the use of an AI system, existing criminal legislation may normally be able to identify the human actor. The more problematic case is when a user provides the system a legitimate goal, but the AI agent independently decides on an illegal or destructive way to achieve that goal. The question then is, whose duty is it, the user, developer, deployer, firm, operator or some other individual that has influence over the system?
The Bharatiya Nyaya Sanhita, 2023 (BNS) which has come into law from 1 July 2024 comprises offences pertaining to AI enabled conduct such as cheating, cheating by personation, producing fake documents, forgery and offences involving electronic records. Sections 318 and 319 are on cheating and cheating by personation. Sections 335 and 336 are on fake documents and forgeries. The act thus offers technology-neutral rules that could apply to numerous AI-assisted offences, but does not develop a distinct framework of accountability for AI autonomous decision-making.

This paper argues that legal responsibility for agentic AI should be kept human-centred, but

ISSN: 2582-6433

become technologically informed. Liability ought to be determined by a structured assessment of who generated the risk, who had control or could have exercised reasonable control over the system, who profited from the operation of the system, what safeguards were available, whether the harmful outcome was foreseeable, and whether reasonable supervision was employed.

RESEARCH PROBLEM AND OBJECTIVES

The rapid rise of agentic Artificial Intelligence (AI) that can plan, decide, use digital resources, and execute tasks autonomously with little human involvement, challenges traditional ideas of legal responsibility. At present, Indian law regulates conduct related to AI under a fragmented framework comprising the Bharatiya Nyaya Sanhita, 2023, the Information Technology Act, 2000, the Bharatiya Sakshya Adhiniyam, 2023, the Digital Personal Data Protection Act, 2023 and nascent AI-governance mechanisms. However, these laws do not expressly establish the manner in which liability should be attributed when an AI system autonomously produces an adverse or unlawful outcome. The primary research question is therefore whether traditional conceptions of purpose, knowledge, control, negligence, foreseeability and causation are adequate to define culpability for autonomous AI activity. In this context, the study aims to study the legal status and characteristics of agentic AI; evaluate the adequacy of existing Indian criminal, civil, technological, data-protection and evidentiary frameworks; analyse relevant judicial developments and institutional responses; and identify gaps in attributing responsibility among developers, deployers, operators and users. The study also aims to present a human-centred, risk-based accountability paradigm that distributes responsibility based on control, foreseeability, benefit, safeguards and capacity for intervention, while guaranteeing that the legal accountability is not undermined by the technological innovation.

CONCEPTUAL FRAMEWORK

Agentic AI is defined as:

Agentic artificial intelligence can be defined as AI that can pursue a goal through a sequence of largely independent decisions and behaviours. It can understand a goal, devise a plan, pick tools, perform activities, evaluate results and adjust its method. The key factor is not just intellect but operational independence. Generative AI mostly creates a result based on a request. Agentic AI might employ the output as a component of an ongoing process of action. This distinction becomes important in a legal sense when the AI has access to other systems and is capable of generating real-world effects. Human-in-the-Loop, Human-on-the-Loop and

ISSN: 2582-6433

Human-out-of-the-Loop. Three governing types are of significant relevance. Human-in-the-loop requires human approval before major actions. Human-on-the-loop lets AI work autonomously, but needs continuous human monitoring and the capacity to intervene. "Human-out-of-the-loop" means AI is able to perform without meaningful human interaction. As a general rule, Indian law should demand at least human-on-the-loop oversight for high-risk artificial intelligence systems, and human-in-the-loop approval for more critical judgements.

LEGAL SYSTEM IN INDIA

Bharatiya Nyaya Sanhita, 2023

Central to the analysis of criminal liability is the BNS. Section 318 talks about cheating while section 319 talks about cheating by personation. Sections 335 and 336 deal with false documents and forgery including electronic data. Section 340.[2] Forged documents or electronic records and their use as genuine. These provisions could apply, potentially, in a situation where an AI agent is purposefully used to deceive, impersonate, manipulate electronic records or facilitate fraud. However, the BNS does not expressly cover a situation where an autonomous AI system independently selects the unlawful means to achieve a human-defined objective. The statute therefore requires interpretative adjustment.

The essential question is whether the necessary intent or knowledge may be imputed to the human actor by virtue of the fact that the human actor used the AI system. That attribution doesn't happen by itself. Criminal culpability is typically based on proof of intention, knowledge, authorisation, wilful disregard or legally accepted carelessness. The BNS rules relating to abetment, conspiracy and attempt might also be relevant if human actors deliberately create or deploy an AI system for criminal objectives.

Information Technology Act, 2000

The Information Technology Act continues to be a major legislation covering computer-related conduct, intermediary duties and electronic conduct. Section 43 [3]deals with civil repercussions of specific unauthorised conduct involving computer resources whereas Section 66 deals with criminal consequences of certain dishonest or fraudulent acts involving computer resources. The statutory basis for intermediary safe harbour subject to conditions defined is provided in Section 79. The Supreme Court's decision in Shreya Singhal v. Union of India, which

[2] Bharatiya Nyaya Sanhita, No. 45 of 2023, §§ 318–19, 335–36, 340 (India).
[3] Information Technology Act, No. 21 of 2000, §§ 43, 66, 79, 79A, 84B–C (India).

ISSN: 2582-6433

recognised the constitutional importance of intermediary liability and read Section 79 together with Article 19(1)(a), remains especially essential. The problem with agentic AI is that the AI system might operate through a number of interconnected services. It may be unclear who the relevant actor is, whether it is the AI developer, infrastructure supplier, model provider, deploying enterprise or end user.

Information Technology (Rules), 2021

The Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021,[4] as modified, prescribe significant intermediary due-diligence duties. The regulatory framework has developed further concerning synthetically generated information and platforms' compliance. While not designed specifically for agentic AI, these Rules suggest that India is moving more responsibility away from individual users and toward digital intermediaries and platforms. A future agentic-AI framework should likewise acknowledge that responsibility can be spread across multiple points in the AI supply chain. The Digital Personal Data Protection Act, 2023 and Rules, 2023

An agentic AI may process vast amounts of personal data when performing tasks. Hence, the Digital Personal Data Protection Act, 2023 will be relevant when AI agents acquire, analyse, store or transfer personal data. The foundation for data protection is critical because an agentic system could potentially access more data than is necessary for the task it has been assigned. This makes the principles of purpose limitation, security safeguards and accountability even more important.

Bharatiya Sakshya Adhiniyam, 2023 (Indian Evidence Act, 2023)

The Bharatiya Sakshya Adhiniyam, 2023 recognises electronic records[5] and sets forth a statutory scheme for their admission. Particularly interesting are the rules on electronic records and certification when it becomes necessary to recreate the actions of an AI agent in a court of law. Agentic AI introduces a new evidentiary problem: the court may have to decide not just what the AI did, but also why it did it, what data it was fed, what commands governed it, what tools it accessed, and what human permits were in place. Consequently, AI logs, system prompts, tool calls, authentication records, model versions, access permissions, and audit trails may be significant evidence.

[4] Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, G.S.R. 139(E), Gazette of India, Extraordinary, Part II, sec. 3(i) (Feb. 25, 2021).
[5] Bharatiya Sakshya Adhiniyam, No. 47 of 2023, §§ 61–63 (India).

ISSN: 2582-6433

CONSTITUTIONAL SETTING

Article 14 ensures non-arbitrariness and equal treatment. Thus, algorithmic decision-making that results in discriminatory outcomes could be subject to constitutional review if there is State intervention. Article 19 safeguards a range of liberties which can be compromised by AI-driven content regulation, automated decision-making and surveillance. The Supreme Court has construed Article 21 widely to safeguard dignity, privacy and decisional autonomy. In Justice K.S. Puttaswamy (Retd.) v. Union of India, the Supreme Court established privacy as a constitutionally protected right under Article 21 and connected safeguards. This has important consequences for AI bots that analyse personal information. Where public authorities implement agentic AI, standards of constitutionality such as legality, proportionality, procedural fairness and accountability should apply.

RESPONSES FROM INSTITUTIONS

Ministry of Electronics and Information Technology (MeitY)

India's digital and AI governance environment is led by MeitY as the primary institutional player. It is responsible for IT legislation, intermediary regulation, data protection and the India AI program. The Ministry's developing approach is an attempt to balance technical innovation and responsibility, rather than instantly enacting a single complete AI statute.

Mission India AI

The IndiaAI Mission is part of India's wider goal to build the infrastructure, capacities, datasets, skills and responsible AI ecosystems for AI. But as more autonomous systems are deployed in the commercial and public domains, the institutional drive for innovation must be matched with improved processes for risk assessment and responsibility.

Judicial Branch

AI is raising more and more questions for the judiciary in India. The Supreme Court's institutional reaction has included a White Paper on AI and Judiciary and, in 2026, a draft framework for the use of AI in courts. Notices issued by the Supreme Court seek views on the Draft Regulations for the Use of AI in Courts, 2026. The Supreme Court has also lately reiterated that the use of AI in adjudication calls for careful oversight, public policy and enforceable regulatory structures rather than unthinking technology acceptance. This judicial evolution is important, as courts might be both consumers of artificial intelligence systems and at the same time adjudicators of conflicts emerging from AI.

ISSN: 2582-6433

JUDICIAL TRENDS & RELEVANT CASE LAW

There is no present, conclusive ruling from the Supreme Court that lays down a comprehensive philosophy of responsibility for agentic AI. Hence, the court analysis should be based on the equivalent concepts already evolved in the technology, privacy, electronic evidence and intermediate instances.

Shreya Singhal v. Union of India (2015)

Shreya Singhal v. Union of India, (2015) 5 SCC 1[6] is a landmark judgement on intermediary responsibility and online communication. The decision reflects the Court's endeavour to reconcile technical realities with constitutional rights. Its concepts are pertinent to agentic AI since intermediary liability cannot be imposed without specifying the legislative basis and the degree of control exercised by the relevant actor.

K.S. Puttaswamy vs Union of India

Privacy was declared as a basic right in Justice K.S. Puttaswamy (Retd.) v. Union of India, (2017) 10 SCC 1.[7] For agentic AI, the judgement gives a constitutional basis for an inquiry into automated processing, monitoring, profiling and autonomous use of data.

CRITICAL ANALYSIS

The advent of agentic Artificial Intelligence (AI) reveals a stark split between classical ideas of legal accountability and increasingly autonomous technological decision-making. Indian criminal law is primarily focused on human behaviour, purpose, knowledge, involvement and causation. However, an agentic AI system can decide intermediate steps and operate without explicit human clearance at each step. And it makes it difficult to assign liability in cases when the adverse result was not explicitly intended or directly ordered by a human agent. The Bharatiya Nyaya Sanhita, 2023 holds technology-neutral crimes that can include numerous AI-enabled acts but does not explicitly provide for a framework for autonomous AI behaviour. Doing so would undermine accepted ideas of individual culpability and mens rea[8] by automatically attaching criminal accountability to developers or users for the simple reason that an AI system committed harm. Equally, letting businesses avoid responsibility by blaming bad action on the "autonomy" of an AI system would create an equally significant

[6] Shreya Singhal v. Union of India, (2015) 5 SCC 1.
[7] Justice K.S. Puttaswamy (Retd.) v. Union of India, (2017) 10 SCC 1.
[8] See generally Ratanlal & Dhirajlal, The Indian Penal Code (LexisNexis ed.).

ISSN: 2582-6433

accountability gap. A more appropriate method is therefore to assess responsibility by reference to control, foreseeability, risk creation, benefit, safeguards and capability to intervene. A developer who builds a system with known vulnerabilities, a deployer who gives too many operational privileges, or an organization that does not implement reasonable monitoring measures could be more liable than a user who reasonably relies on a system without knowing its risks. The "black-box" nature of advanced artificial intelligence systems also makes the situation worse, as it can be hard for judges to trace how a certain decision was made. Therefore, it is imperative to protect audit trails, system logs, data provenance, recordings of human intervention and expert testimony under the Bharatiya Sakshya Adhiniyam, 2023[9]. Moreover, unrestricted culpability of creators may act as a deterrent to technology progress, whereas no liability can leave victims without effective redress. The law therefore needs to progress toward a paradigm of accountability that is appropriate, risk-based and human-centred, rather than regarding AI as a mere tool or as an autonomous legal person. The guiding idea should be that technical autonomy cannot itself be a shield to accountability. When humans or organisations intentionally outsource important decision-making powers to an AI system, they must retain matching roles of monitoring, risk assessment and intervention. This strategy preserves innovation and ensures that the rising autonomy of AI does not lead to less accountability for those who design, implement, control or benefit from it.

PROPOSED LEGAL RESPONSIBILITY MODEL

A viable framework for evaluating legal responsibility for agentic Artificial Intelligence (AI) should move beyond the traditional premise that accountability should lie exclusively with the person who directly does the detrimental conduct. Rather, accountability should be framed within a human-centred, risk-based and control-oriented approach, as agentic artificial intelligence systems can plan freely, make intermediate decisions, access digital resources, and perform approved activities. The first issue in this approach should be authorisation, namely who approved the AI system to do the relevant activity and specified the objectives within which it operated. The second consideration should be control looking at who created, configured, deployed, monitored or had the authority to intervene in the operation of the system. Third, foreseeability should be a factor in whether the harm that transpired could reasonably have been predicted, based on the system's capabilities, recognised limitations and operating environment. Fourth, benefit and risk should be created, not just for the individual or

[9] Bharatiya Sakshya Adhiniyam, No. 47 of 2023, §§ 39, 61–63 (India).

ISSN: 2582-6433

organization who stands to gain commercially or institutionally but in the knowledge that others will be exposed to technical risk. Fifth, courts should evaluate the sufficiency of protections, such as cybersecurity precautions, access limitations, monitoring methods, testing, oversight by humans, and emergency intervention processes. Finally, one should analyse the ability to intervene and if the actor concerned might have reasonably recognised, prevented or stopped the detrimental act. These factors would enable responsibility to be assigned proportionally across developers, model providers, deployers, operators and end users rather of automatically assigning accountability to one actor. Such a framework will also differentiate between purposeful misapplications and irresponsible deployment as well as truly unexpected system failure, hence maintaining the core values of criminal liability and justice. Crucially, the approach being offered does not depend on AI being considered an independent legal entity. Instead, it considers AI autonomy as a factor influencing the extent of human accountability. The idea is that more autonomy and more risk should go together with more duties of oversight, documentation and accountability. This would enable Indian law to handle autonomous AI-related harm without unduly hampering technical progress while ensuring that the delegation of decision-making to AI does not become a method of eschewing legal responsibility.

STRONG RECOMMENDATIONS

India needs a holistic framework for regulating agentic AI, not limited to existing technology-neutral rules but rather one that is risk-based and human-centric. First, the Government should consider creating specific statutory measures to deal with high-risk and autonomous artificial intelligence systems, with explicit definitions of the duties of developers, providers, deployers, operators and users. Such legislation should not create an autonomous legal personality of AI, but should introduce responsibilities according to control, foreseeability, risk creation, benefit and capability to intervene. Secondly, high-risk agentic artificial intelligence systems in sectors such as healthcare, banking, financial services, employment, law enforcement and critical infrastructure should undergo required pre-deployment risk assessments, independent testing and frequent compliance audits. Third, there should be a requirement of real oversight by humans in critical judgements. Organisations should guarantee that human intervention is technically feasible, timely and effective, in particular where an AI agent can autonomously perform financial transactions, access sensitive information or impact individual rights. Fourth, developers and deployers should be expected to preserve tamper-resistant audit trails, including recordings of system commands, data inputs, tool usage, permissions, significant decisions, human interventions and material system changes. Such recordings will assist courts in

ISSN: 2582-6433

determining causation and liability under the Bharatiya Sakshya Adhiniyam, 2023. Fifth, India should set up a clear AI incident-reporting process, which requires major autonomous-system failures, security breaches and damaging judgements to be reported promptly to the relevant regulatory authorities. Sixth, the principle of least privilege must be mandatory for agentic systems such that AI agents are only given the rights required to fulfil their assigned jobs. Seventh, there should be unambiguous responsibilities of care, supervision and cyber-security for businesses using high-risk AI, with suitable consequences for reckless deployment or failing to put in place sufficient protections. Eighth, regulators should work with technological experts, legal experts, industry stakeholders, and civil society to produce sector-specific AI guidelines. Ninth, Indian courts, prosecutors and lawyers should be given specialised training in AI architecture, algorithmic decision-making, digital evidence, system logs and expert testimony so that technological complexity does not hinder successful adjudication. Finally, India should create an inter-regulatory AI coordination framework that can monitor emerging hazards and periodically revise regulatory norms as technology evolves. Such efforts should be supported by protections against over-regulation, so that innovation is not excessively curtailed. Most critically, Indian AI governance must establish the principle that autonomy does not negate accountability: when individuals or organisations intentionally use systems that are capable of independent action, they must retain commensurate responsibilities for reasonable supervision, risk management, transparency and intervention. This will give industry greater confidence, individuals stronger protection and a stable legal basis for the responsible development of agentic AI in India.

CONCLUSION

Agentic artificial intelligence marks a radical departure from AI as a passive computational tool to AI as an increasingly autonomous operational actor. Its capacity to plan, select actions, use tools and perform tasks raises legal difficulties that cannot be totally answered through conventional software regulation. Indian law already has a number of measures that may be used to mitigate harm caused by AI. The Bharatiya Nyaya Sanhita, 2023 contains technology neutral criminal laws. The Information Technology Act regulates computer related conduct and intermediaries. The Bharatiya Sakshya Adhiniyam provides for recognition of electronic evidence. The Digital Personal Data Protection Act and Rules lay down obligations in relation to personal data. Sectoral regulators may prescribe additional standards. Yet these regulations do not provide a comprehensive framework for allocating liability when an AI system operates with a high degree of operational autonomy.

ISSN: 2582-6433

The right answer is not to make AI a legal person. Such a stance risks hiding the humans and organisations who build, operate and benefit from artificial intelligence (AI) technology. Instead, India should embrace a human-centred, risk-based and control-sensitive approach to AI responsibility. The guiding concept should be that technical autonomy does not obviate human accountability. No person or organization who wilfully designs, deploys or oversees an autonomous system should be able to escape legal liability only because an algorithm took the initial decision. At the same time, regulation cannot place endless culpability on developers for every unanticipated AI result. Responsibility should be linked to control, foreseeability, risk generation, benefit, safeguards and capacity for intervention. The proposed AI Responsibility Attribution Model offers a practical basis for this approach. By assessing power, control, foreseeability, benefit, safeguards and intervention, responsibility can be divided according to the participation of each person. The developing regulatory landscape in India indicates that at least AI governance is progressing beyond abstract policy dialogue. With AI being used more and more in business and government, India's data-protection law is being put into practice and the Supreme Court is moving on with its work on the use of AI in courts, legal institutions are entering a new phase of technological governance.

Thus, the fundamental legal question of agentic AI is not whether robots will substitute for human beings as legal actors. The question is whether law can continue to detect the human responsibility embodied in more autonomous technical systems? Thus, the regulatory purpose of India should not be technical prohibition nor unfettered technology freedom. It should be responsible autonomy – enabling artificial intelligence to develop and perform beneficial functions but guaranteeing that autonomy is associated by traceability, oversight by humans, proportional liability, transparency and effective remedies.

Delegating decision-making to artificial intelligence can never be a delegation away from legal accountability. Only if India adheres to this premise can it build an AI ecosystem that is inventive, constitutionally compatible, economically profitable and legally accountable.