LAWFOYER INTERNATIONAL JOURNAL OF DOCTRINAL LEGAL RESEARCH

(ISSN: 2583-7753)

Volume 3 | Issue 1

2025

CRIMINAL ACCOUNTABILITY FOR AI: MENS REA, ACTUS REUS, AND THE CHALLENGES OF AUTONOMOUS SYSTEMS

Akanksha Priya*

I. ABSTRACT

Criminal accountability for harms caused by artificial intelligence systems presents profound challenges for traditional legal frameworks. The mens rea and actus reus pillars of Indian criminal jurisprudence face conceptual strains when applied to algorithmic decision-making. AI systems lack human-like mental states and discrete physical acts that form the foundation of criminal culpability. The Bharatiya Nyaya Sanhita, 2023 and other Indian laws inadequately address these accountability gaps. This article examines the conceptual and practical obstacles to AI criminal liability under current Indian legal frameworks. It analyzes relevant provisions of the Bharatiya Nyaya Sanhita and identifies their limitations in AI contexts. The article explores comparative regulatory approaches from the European Union, United States, United Kingdom, Singapore, and other jurisdictions. The article concludes by proposing legal and policy recommendations for India to address AI criminal accountability challenges. These include establishing AI-specific legislation, incorporating risk-based obligations, mandating human oversight for high-risk applications, and developing specialized enforcement capacities. The article emphasizes the urgent need for Indian legal frameworks to evolve beyond anthropocentric paradigms and accommodate the distinctive characteristics of artificial intelligence. Only through such evolution can India establish effective and legitimate mechanisms for attributing criminal responsibility when AI systems cause harm.

* Pursuing LLM in Criminal Law From Amity University, Batch 2024-2025

 (ISSN: 2583-7753)

II. KEYWORDS

Artificial Intelligence, Criminal Liability, Mens Rea, Actus Reus, Indian Criminal Law.

III. INTRODUCTION

A. Context of AI systems and criminal liability challenges

Artificial Intelligence systems are transforming from experimental projects to everyday tools at breakneck speed. These systems now make critical decisions across healthcare, transportation, finance and law enforcement domains. Traditional criminal liability frameworks face severe strain when applied to harms caused by AI systems. The criminal law's foundation rests on concepts designed for human actors with human cognitive abilities. AI systems operate through fundamentally different mechanisms of algorithms and neural networks.[1]

The attribution of criminal responsibility becomes profoundly challenging when AI systems cause harm. Indian criminal jurisprudence centers on mens rea and actus reus as twin pillars of liability. Both elements assume human agency, consciousness and moral culpability. The mens rea requirement creates particular difficulties for AI accountability. An AI system lacks mental states in the conventional sense understood by criminal law. Yet these systems make autonomous decisions that can lead to harmful outcomes. This creates a accountability gap that current legal frameworks struggle to address.[2]

The Bharatiya Nyaya Sanhita, 2023 continues this traditional approach. Section 2 defines acts, intentions and knowledge in distinctly human terms. It conceptualizes offenses as requiring human-like mental states. This approach becomes problematic when applied to algorithmic decision-making. The criminal law must evolve to accommodate

[1] Stuart Russell & Peter Norvig, ARTIFICIAL INTELLIGENCE: A MODERN APPROACH 27-30 (4th ed. 2020).
[2] Gabriel Hallevy, When Robots Kill: Artificial Intelligence under Criminal Law 15-24 (Ne. Univ. Press 2013).

 (ISSN: 2583-7753)

autonomous systems while maintaining its core functions of deterrence, retribution and public safety.[3]

Indian regulatory frameworks addressing AI responsibility remain in nascent stages. The Information Technology Act, 2000 fails to adequately address algorithmic accountability. Specialized AI regulations remain under development. The Supreme court in Karmanya Singh Sareen v. Union of India acknowledged the growing need for technology-specific legal frameworks. This regulatory gap leaves victims, developers and users in legal uncertainty.[4]

The vicarious liability doctrine offers one potential path forward. Under this approach, creators or operators of AI systems would bear responsibility for harms. But this stretches traditional vicarious liability principles beyond recognition. Indian courts have shown reluctance to expand vicarious liability without clear legislative mandate. The Delhi High Court in Christian Louboutin SAS v. Nakul Bajaj emphasized this judicial restraint.[5]

Global approaches provide instructive models for Indian jurisprudence. The European Union has proposed a risk-based AI regulatory framework. This creates varying obligations based on an AI system's potential harm. The United States employs a sectoral approach focusing on high-risk domains. Singapore emphasizes technical requirements for explainability and human oversight. These frameworks balance innovation with robust accountability mechanisms.[6]

B. Research Questions

1. How do the mens rea and actus reus requirements of Indian criminal law conceptually map onto the distinctive decision-making processes of artificial intelligence systems?

[3] Bharatiya Nyaya Sanhita, 2023, § 2, No. 45, Acts of Parliament, 2023 (India).
[4] Karmanya Singh Sareen v. Union of India, (2018) 1 SCC 560.
[5] Christian Louboutin SAS v. Nakul Bajaj, 253 (2018) DLT 728.
[6] Ryan Calo, Artificial Intelligence Policy: A Primer and Roadmap, 51 U.C. DAVIS L. REV. 399, 410-15 (2017).

2. To what extent do existing provisions of the Bharatiya Nyaya Sanhita, 2023 and other Indian laws enable or constrain criminal liability attribution for harms caused by AI systems?
3. What lessons can India draw from comparative international approaches to regulating criminal liability for artificial intelligence, and how can these insights inform the development of effective and contextually appropriate legal frameworks?

C. Research Objectives

1. Analyze the conceptual foundations of mens rea and actus reus in Indian criminal jurisprudence and identify the specific challenges in applying these concepts to AI systems that lack human-like mental states and discrete physical actions.
2. Critically examine relevant provisions of the Bharatiya Nyaya Sanhita and other key Indian legislation to assess their adequacy and limitations in establishing effective accountability frameworks for AI-related crimes.
3. Conduct a comparative analysis of AI criminal liability approaches in key jurisdictions such as the European Union, United States, United Kingdom, and Singapore to identify promising regulatory strategies and evaluate their suitability for adaptation to the Indian legal context.

IV. TRADITIONAL CRIMINAL LIABILITY FRAMEWORK

A. Components of criminal liability: mens rea and actus reus

Criminal liability in India rests fundamentally on two essential pillars: mens rea and actus reus. This duality forms the bedrock of criminal jurisprudence across most legal systems. Mens rea represents the guilty mind or mental element. Actus reus constitutes the physical element or prohibited conduct. Both elements must coexist for criminal liability to attach in most offenses.[7]

[7] K.D. Gaur, CRIMINAL LAW: CASES AND MATERIALS 52-58 (8th ed. 2020).

The concept of mens rea encompasses various mental states. It includes intention, knowledge, recklessness, and negligence in descending order of culpability. The Bharatiya Nyaya Sanhita, 2023 reflects these gradations through terms like "voluntarily," "intentionally," and "knowingly." Section 33 defines voluntariness as causing an effect by means intended or known to be likely. This definition captures the essence of conscious moral choice.[8]

Indian courts consistently uphold the necessity of mens rea. The Supreme Court in Kartar Singh v. State of Punjab emphasized criminal law's foundation on moral culpability. Mental intent transforms a physically harmful act into a crime deserving punishment. Absence of mens rea generally precludes criminal liability except in strict liability offenses. Even these remain rare exceptions rather than the norm in Indian jurisprudence.[9]

The actus reus component represents the external manifestation of criminality. It may constitute an affirmative act, an omission where duty exists, or possession of prohibited items. The Bharatiya Nyaya Sanhita defines "act" in Section 2(1) as encompassing a series of acts. Section 2(25) similarly defines "omission" as including a series of omissions. This comprehensive approach captures the multifaceted nature of prohibited conduct.[10]

Beyond mere bodily movement, actus reus must occur voluntarily. Involuntary actions like reflexes, convulsions or movements during unconsciousness lack the voluntary character required. The Delhi High Court in Gauri Shankar v. State affirmed this principle. External forces compelling physical movement negate criminal responsibility. This reinforces the connection between act and will central to criminal liability.[11]

The causation element links the actus reus to harmful consequences. Legal causation differs from mere factual causation. Intervening acts may break the causal chain. The Supreme Court in Basdev v. State of Pepsu articulated a test of foreseeability. A defendant

[8] Bharatiya Nyaya Sanhita, 2023, § 33, No. 45, Acts of Parliament, 2023 (India).
[9] Kartar Singh v. State of Punjab, (1994) 3 SCC 569.
[10] Bharatiya Nyaya Sanhita, 2023, § 2(1), § 2(25), No. 45, Acts of Parliament, 2023 (India).
[11] Gauri Shankar v. State, 2015 SCC OnLine Del 9356.

remains liable for reasonably foreseeable consequences of their actions. This causation requirement ensures proportionate attribution of responsibility.[12]

Concurrence between mens rea and actus reus proves essential for liability. The guilty mind must actuate the guilty act. Temporal coincidence typically suffices in most cases. In continuing offenses, the mens rea must exist during the prohibited conduct. The Supreme Court in State of Maharashtra v. Mayer Hans George emphasized this principle. A later-formed intent cannot retroactively criminalize an earlier innocent act.[13]

Indian criminal jurisprudence recognizes certain exceptions to the mens rea requirement. The Bharatiya Nyaya Sanhita provides specific exceptions in Chapter III. These include mistakes of fact, acts of judges, accidents, and unsoundness of mind. Such exceptions acknowledge circumstances where moral culpability is absent despite harmful consequences. This reflects criminal law's moral foundation beyond mere harm causation.[14]

The mens rea-actus reus framework serves crucial societal functions. It distinguishes criminal from civil wrongs through moral culpability. This framework limits punishment to blameworthy conduct. It promotes fairness by punishing according to culpability levels. The framework also serves deterrent functions by targeting conscious choices. These principles remain foundational despite evolving interpretations across jurisdictions.[15]

B. Bhartiya Nyaya Sanhita provisions relevant to AI contexts

The Bharatiya Nyaya Sanhita, 2023 replaces the colonial-era Indian Penal Code with modernized provisions. This comprehensive legislation retains fundamental criminal law principles while introducing contemporary elements. Several provisions hold

[12] Basdev v. State of Pepsu, AIR 1956 SC 488.
[13] State of Maharashtra v. Mayer Hans George, AIR 1965 SC 722.
[14] Bharatiya Nyaya Sanhita, 2023, Chapter III, No. 45, Acts of Parliament, 2023 (India).
[15] V.S. Malimath, COMMITTEE ON REFORMS OF CRIMINAL JUSTICE SYSTEM, GOVERNMENT OF INDIA 170-175 (2003).

particular relevance for AI systems and their potential criminal liability. These provisions merit careful examination through the lens of artificial intelligence applications.[16]

Section 2 of the Sanhita provides definitional foundations critical to AI contexts. It defines "act" to include "a series of acts" and similarly defines "omission." AI systems operate through continuous algorithmic processes rather than discrete actions. This definitional approach potentially encompasses the operational continuum of AI systems. Yet the Sanhita presumes human agency throughout its definitions. This creates interpretative challenges for AI accountability.[17]

The Sanhita's definition of "person" under Section 2(26) includes "any company or association or body of persons, whether incorporated or not." This expansive definition might conditionally extend to AI systems. However, judicial interpretation will determine whether algorithmic entities qualify as "persons" under this provision. The absence of explicit technological references creates ambiguity. Courts must address whether AI systems constitute "persons" for criminal liability purposes.[18]

Section 3(5) extends the Sanhita's application to offenses committed by "any person in any place without and beyond India committing offence targeting a computer resource located in India." This provision appears particularly relevant to cloud-based AI systems. An AI system physically located abroad could face liability for harming Indian computer resources. This creates potential extraterritorial application to cross-border AI operations. Enforcement mechanisms for such provisions remain underdeveloped.[19]

Section 39 introduces the legal fiction of "deemed knowledge" in certain contexts. This provision potentially addresses AI systems' knowledge attribution challenges. Courts might apply this provision to impute knowledge to AI developers or operators. The

[16] Bharatiya Nyaya Sanhita, 2023, No. 45, Acts of Parliament, 2023 (India).
[17] Bharatiya Nyaya Sanhita, 2023, § 2(1), § 2(25), No. 45, Acts of Parliament, 2023 (India).
[18] Bharatiya Nyaya Sanhita, 2023, § 2(26), No. 45, Acts of Parliament, 2023 (India); see also State Trading Corp. of India v. Commercial Tax Officer, AIR 1963 SC 1811 (discussing personhood of non-human entities).
[19] Bharatiya Nyaya Sanhita, 2023, § 3(5), No. 45, Acts of Parliament, 2023 (India).

fiction of "reason to believe" could bridge gaps between algorithmic decision-making and human awareness. This interpretative approach would require judicial creativity beyond the provision's literal text.[20]

The Sanhita recognizes vicarious liability principles through Section 190. It states that "when an offence is committed by any member of an unlawful assembly... every person who... is a member of the same assembly, is guilty of that offence." This collectivist approach might extend to AI development teams or operational groups. Courts could potentially hold human teams collectively responsible for AI-caused harms.[21]

Corporate criminal liability finds recognition in Section 2(26) read with various substantive provisions. AI systems typically operate within corporate structures as products or services. The Sanhita's corporate liability framework could attribute AI-caused harms to corporate entities. This potentially circumvents the challenge of establishing an AI system's direct mens rea. Corporate knowledge or intent might substitute for algorithmic mental states.[22]

Section 61(1) addresses criminal conspiracy when "two or more persons agree with the common object to do, or cause to be done an illegal act." AI systems often involve multiple stakeholders in development and deployment. This provision could apply to development teams creating AI with foreseeable harmful capabilities. The agreement element would require establishing shared human intent behind AI design or deployment.[23]

The Sanhita's negligence-based offenses offer promising avenues for AI accountability. Section 106 punishes death caused by negligence. This could extend to deaths resulting from AI system failures. The provision's negligence standard bypasses intent requirements problematic for AI contexts. Developers or operators failing to take

[20] Bharatiya Nyaya Sanhita, 2023, § 39, No. 45, Acts of Parliament, 2023 (India).
[21] Bharatiya Nyaya Sanhita, 2023, § 190, No. 45, Acts of Parliament, 2023 (India).
[22] Iridium India Telecom Ltd. v. Motorola Inc., (2011) 1 SCC 74 (discussing attribution of mens rea to corporations).
[23]Bharatiya Nyaya Sanhita, 2023, § 61(1), No. 45, Acts of Parliament, 2023 (India).

reasonable precautions with high-risk AI applications could face liability under this framework.[24]

Regulatory offenses within the Sanhita present another pathway. Section 353(1)(d) criminalizes "publishing false or misleading information jeopardising the sovereignty, unity and integrity or security of India." AI systems generating or amplifying harmful misinformation might trigger this provision. The focus on harmful effects rather than mental states accommodates AI operations. This effects-based approach suits technological contexts where intent proves elusive.[25]

Section 125 criminalizes "doing any act so rashly or negligently as to endanger human life." This could apply to deploying insufficiently tested AI in critical contexts. The provision emphasizes dangerous conduct rather than harmful results. This enables earlier intervention before AI systems cause actual harm. The preventative function serves important safety purposes in emerging technologies.[26]

Abetment provisions in Sections 45-60 potentially capture human facilitation of AI harms. Developers knowingly creating AI with dangerous capabilities might face abetment charges. The provisions distinguish instigation, conspiracy, and aid forms of abetment. This nuanced approach accommodates various human roles in AI development and deployment. Intent requirements focus on human rather than algorithmic mental states.[27]

The "general exceptions" in Chapter III could provide defenses in AI contexts. Section 18 exempts "accident or misfortune" without criminal intent. AI systems causing unforeseeable harms might qualify for this exception. Similarly, Section 19 exempts acts done "without criminal intention... in good faith... to avoid other harm." This might protect good-faith AI deployments causing unforeseen consequences.[28]

[24]Bharatiya Nyaya Sanhita, 2023, § 106, No. 45, Acts of Parliament, 2023 (India).
[25] Bharatiya Nyaya Sanhita, 2023, § 353(1)(d), No. 45, Acts of Parliament, 2023 (India).
[26] Bharatiya Nyaya Sanhita, 2023, § 125, No. 45, Acts of Parliament, 2023 (India).
[27]Bharatiya Nyaya Sanhita, 2023, §§ 45-60, No. 45, Acts of Parliament, 2023 (India)
[28]. Bharatiya Nyaya Sanhita, 2023, §§ 18-19, Chapter III, No. 45, Acts of Parliament, 2023 (India).

 (ISSN: 2583-7753)

Section 111 on "organised crime" defines continuing unlawful activities including "cyber-crimes, trafficking of persons, drugs, weapons or illicit goods or services." Advanced AI systems could potentially facilitate such organized criminal activities. The provision's focus on systematic operations rather than individual acts suits algorithmic contexts. Enhanced penalties reflect the increased harm potential of technologically-enabled organized crime.[29]

The introduction of "community service" as punishment under Section 4(f) offers an additional sentencing option. This could provide proportionate responses for less culpable AI-related offenses. Corporate entities responsible for negligent AI deployments might receive remedial community service orders. This allows for rehabilitative rather than purely punitive approaches to AI accountability.[30]

C. The foundation of moral culpability in criminal law

Moral culpability forms the essential bedrock of criminal law in India and most legal systems worldwide. Criminal law addresses wrongs considered morally reprehensible by society. This moral dimension distinguishes criminal liability from civil liability in fundamental ways. The concept of deserved punishment emerges directly from moral blameworthiness. Legal systems impose criminal sanctions only when moral culpability exists.[31]

The Supreme Court in Kartar Singh v. State of Punjab emphasized this moral foundation. Justice K. Ramaswamy observed that criminal liability attaches to choices made by morally autonomous agents. Such choices must occur with sufficient awareness of circumstances and consequences. The Court linked punishment justification directly to moral responsibility. This perspective reflects deep philosophical roots in Indian jurisprudence.[32]

[29] Bharatiya Nyaya Sanhita, 2023, § 111, No. 45, Acts of Parliament, 2023 (India).
[30] Bharatiya Nyaya Sanhita, 2023, § A(f), No. 45, Acts of Parliament, 2023 (India).
[31] Glanville Williams, CRIMINAL LAW: THE GENERAL PART 29-30 (2d ed. 1961).
[32] Kartar Singh v. State of Punjab, (1994) 3 SCC 569, ¶ 42.

Criminal law's moral foundation explains why Indian courts rarely recognize strict liability. Traditional offenses require moral culpability through mens rea requirements. Strict liability remains confined to regulatory offenses with limited penalties. Even these regulatory exceptions often retain elements of moral judgment.

Various theoetical justifications support this moral foundation. Retributive theory views punishment as deserved for morally culpable choices. Deterrence theory assumes moral agents capable of being influenced by threatened consequences. Rehabilitative approaches presume moral capacity for personal reformation. Expressionist theories emphasize punishment as communicating moral condemnation. All these frameworks presuppose moral culpability.[33]

The proportionality principle further reflects criminal law's moral foundation. More culpable mental states warrant greater punishment under Indian sentencing principles. Knowledge-based offenses typically carry heavier penalties than negligence-based ones. The Bharatiya Nyaya Sanhita reflects this graduated approach through escalating punishments. This calibration directly connects punishment severity to moral blameworthiness.[34]

Moral culpability explains the criminal law's numerous defenses and exceptions. Insanity defenses recognize diminished moral responsibility through impaired cognition. Necessity and duress defenses acknowledge constrained moral agency. Mistake defenses acknowledge diminished culpability through factual misapprehension. These exceptions confirm moral culpability as the foundational prerequisite. The Supreme Court in Gurbachan Singh v. State of Punjab emphasized this principle.[35]

Ancient Indian legal traditions consistently recognized moral culpability as essential. Dharmasastras distinguished between intentional and unintentional harms. Manusmriti prescribed different punishments based on mental elements. This moral foundation

[33] Paul H. Robinson, DISTRIBUTIVE PRINCIPLES OF CRIMINAL LAW: WHO SHOULD BE PUNISHED HOW MUCH? 109-114 (2008).
[34] Bharatiya Nyaya Sanhita, 2023, §§ 101-103, No. 45, Acts of Parliament, 2023 (India).
[35] Gurbachan Singh v. State of Punjab, (1980) 2 SCC 565.

persisted through centuries of legal evolution. Modern Indian criminal jurisprudence maintains continuity with these historic moral underpinnings.[36]

The foundation of moral culpability creates significant challenges for AI accountability. Artificial systems lack consciousness, free will, or moral agency in human sense. They cannot experience guilt or remorse for outcomes. Their decision-making processes differ fundamentally from human moral reasoning. This creates profound tensions when applying traditional criminal frameworks to AI systems.[37]

V. CONCEPTUAL CHALLENGES IN APPLYING CRIMINAL LAW TO AI

A. The mens rea challenge: Can AI systems form intent?

The mens rea requirement poses perhaps the most significant obstacle to AI criminal liability. Mens rea traditionally encompasses conscious mental states like intention, knowledge, and recklessness. AI systems process information and make decisions through fundamentally different mechanisms. They lack consciousness, emotions, or subjective awareness in any human sense. Neural networks operate through mathematical calculations without comprehending their actions.[38]

Modern criminal law presupposes moral agency rooted in cognitive awareness. The Indian Supreme Court in Basdev v. State of Pepsu emphasized mens rea as flowing from moral choice. AI systems lack this capacity for moral discernment. They cannot distinguish right from wrong in any meaningful sense. Their programming optimizes for specific outcomes without moral comprehension. This absence of moral understanding creates a conceptual mismatch with criminal liability.[39]

[36] Werner Menski, HINDU LAW: BEYOND TRADITION AND MODERNITY 125-130 (2003).
[37] Gabriel Hallevy, THE CRIMINAL LIABILITY OF ARTIFICIAL INTELLIGENCE ENTITIES - FROM SCIENCE FICTION TO LEGAL SOCIAL CONTROL, 4 AKRON INTELL. PROP. J. 171, 175-179 (2010).
[38] Stuart Russell & Peter Norvig, ARTIFICIAL INTELLIGENCE: A MODERN APPROACH 32-58 (4th ed. 2020).
[39] Basdev v. State of Pepsu, AIR 1956 SC 488.

AI systems operate through goals, rewards, and penalties programmed by humans. They optimize behavior accordingly without understanding moral implications. A self-driving car maximizing safety parameters lacks comprehension of why safety matters. This algorithmic pursuit differs fundamentally from human intentionality. The distinction challenges traditional intent concepts requiring purposive awareness. Courts must confront this divergence between algorithmic goal-pursuit and human intentionality.[40]

Machine learning systems develop behavioral patterns through data analysis rather than conscious choice. They identify correlations and optimize decision pathways without understanding causation. Their "learning" differs fundamentally from human learning imbued with meaning. This statistical approach to decision-making lacks the cognitive elements underlying mens rea. The Supreme Court's mens rea jurisprudence presumes human-like comprehension entirely absent in AI.[41]

The gradations of mens rea further complicate AI accountability. Indian criminal law distinguishes between intention, knowledge, and negligence. These distinctions reflect degrees of moral culpability. AI systems cannot experience these differentiated mental states. Their decision matrices calculate probabilities without subjective awareness. Importing these concepts into algorithmic contexts requires problematic anthropomorphizing. Courts must avoid misleading analogies between AI processes and human cognition.[42]

Some scholars propose functional equivalence approaches to AI mens rea. Under this view, AI systems exhibiting behavior patterns analogous to human intent functionally possess mens rea. This approach prioritizes observable outcomes over unobservable mental states. Professor Gabriel Hallevy advocates this perspective for practical accountability. Yet critics note this sidesteps the core moral basis of criminal liability.[43]

[40] Ryan Calo, Robotics and the Lessons of Cyberlaw, 103 CALIF. L. REV. 513, 538-545 (2015).
[41] State of Maharashtra v. Mohd. Yakub, (1980) 3 SCC 57.
[42] P.S.R. Sadhanantham v. Arunachalam, (1980) 3 SCC 141.
[43] Gabriel Hallevy, THE CRIMINAL LIABILITY OF ARTIFICIAL INTELLIGENCE ENTITIES - FROM SCIENCE FICTION TO LEGAL SOCIAL CONTROL, 4 AKRON INTELL. PROP. J. 171, 175-179 (2010).

Another approach rejects anthropomorphizing AI entirely. This perspective locates mens rea exclusively in human developers or operators. The focus shifts to foreseeability of harmful outcomes by human actors. This approach preserves criminal law's moral foundations while addressing AI harms. The Karnataka High Court employed similar reasoning in State v. Krishna Pillai regarding corporate criminal liability.[44]

Determining appropriate mens rea standards for AI requires examining specific implementation contexts. Medical diagnosis systems demand different standards than autonomous vehicles. Financial trading algorithms warrant different approaches than content moderation systems. Context-specific analysis acknowledges varying risk profiles and societal impacts. This nuanced approach avoids one-size-fits-all solutions inappropriate for diverse AI applications.[45]

The mens rea challenge ultimately reflects AI's distinctive ontological status. AI systems are neither moral agents nor passive tools. They occupy an unprecedented intermediate categroy. Their capacity for adaptive learning and decision-making exceeds traditional tools. Yet they lack fundamental attributes of moral agency underlying criminal responsibility. This ontological uniqueness demands reconsideration of traditional mens rea frameworks.[46]

B. The actus reus challenge: Identifying the "guilty act" in autonomous systems

While mens rea presents significant challenges, identifying the relevant actus reus in AI contexts proves equally problematic. Traditional criminal law conceptualizes the actus reus as a voluntary physical act or omission. AI systems operate through computational processes rather than bodily movements. These processes involve complex interactions across distributed components. Locating a discrete "act" becomes inherently difficult.[47]

[44] State v. Krishna Pillai, 1978 CrLJ 701 (Kant.).
[45] Matthew U. Scherer, Regulating Artificial Intelligence Systems: Risks, Challenges, Competencies, and Strategies, 29 HARV. J.L. & TECH. 353, 362-365 (2016).
[46] David C. Vladeck, Machines Without Principals: Liability Rules and Artificial Intelligence, 89 WASH. L. REV. 117, 120-126 (2014).
[47] A.P. Simester & G.R. Sullivan, CRIMINAL LAW: THEORY AND DOCTRINE 87-92 (7th ed. 2019).

The voluntary requirement in actus reus creates particular difficulties with AI systems. Voluntariness traditionally implies human bodily control and choice. AI systems execute algorithms deterministically yet adaptively. Their operations lack volition in any human sense. Yet autonomy distinguishes them from passive tools. They make independent decisions based on environmental inputs. This creates an ontological mismatch with traditional actus reus concepts.[48]

AI decision-making typically involves probabilistic calculations across millions of parameters. These calculations happen rapidly across distributed hardware. The "act" occurs across numerous computational steps rather than discrete physical movements. The Supreme Court in State of Maharashtra v. M.H. George conceptualized acts as unitary events. This framework poorly accommodates distributed computational processes spanning space and time.[49]

The challenge extends to identifying precisely when an AI "act" occurs. Does it arise during programming, during learning, or during operational decision-making? An autonomous vehicle's collision might trace to code written years earlier. It might equally trace to learning processes occurring months prior. The temporal dispersal of computational causality defies traditional actus reus timing concepts. The Bharatiya Nyaya Sanhita's definition of "act" inadequately addresses this temporal complexity.[50]

Omission liability raises additional complexities in AI contexts. Criminal omissions require legal duties to act. AI systems lack legal personhood and corresponding duties. Yet their operational parameters define functional responsibilities. An AI medical diagnosis system failing to identify cancer resembles human diagnostic negligence. Courts must determine whether such functional roles create duty-based obligations without personhood. The law currently provides limited guidance on this question.[51]

[48] State of Maharashtra v. Sindhi, (1975) 1 SCC 647 (discussing voluntariness requirement in criminal acts).
[49] State of Maharashtra v. M.H. George, AIR 1965 SC 722.
[50] Bharatiya Nyaya Sanhita, 2023, § 2(1), No. 45, Acts of Parliament, 2023 (India).
[51] Jack B. Balkin, The Path of Robotics Law, 6 CALIF. L. REV. CIRCUIT 45, 51-52 (2015).

The causation element of actus reus presents particular difficulties with AI systems. Multiple actors contribute to AI outcomes across development, deployment, and operation. Software developers, data scientists, corporate managers and end-users all influence system behavior. Isolating causal responsibility becomes exceedingly complex. Traditional but-for and proximate cause tests struggle with these distributed causal chains. The Supreme Court in Nidhi Kaim v. State of M.P. addressed causal complexity in technological contexts.[52]

Many AI harms result from emergent behaviors rather than programmed instructions. Machine learning systems develop novel approaches through training. These approaches may diverge from developer intentions or expectations. The resulting behaviors emerge from complex interactions between code, data, and environment. This emergent quality challenges traditional actus reus conceptions focusing on discrete, predictable human actions.[53]

The continuous nature of AI operation further complicates actus reus identification. Many AI systems operate continuously, constantly processing information and making decisions. They lack discrete operational episodes comparable to human actions. This continuity challenges criminal law's focus on distinct criminal acts. The Bharatiya Nyaya Sanhita defines "act" to include "a series of acts" but this inadequately captures AI's operational continuity.[54]

Different AI architectures present varying actus reus challenges. Rules-based systems follow explicit instructions programmed by humans. Machine learning systems develop behavioral patterns through data exposure. Deep learning systems operate through inscrutable neural networks. Each architecture requires different approaches to actus

[52] Nidhi Kaim v. State of Madhya Pradesh, (2017) 4 SCC 1.
[53] Ryan Abbott, The Reasonable Computer: Disrupting the Paradigm of Tort Liability, 86 GEO. WASH. L. REV. 1, 7-12 (2018).
[54] Bharatiya Nyaya Sanhita, 2023, § 2(1), No. 45, Acts of Parliament, 2023 (India).

reus identification. A unified framework may prove conceptually impossible given these architectural variations.[55]

The challenge compounds with multi-agent AI systems involving numerous interacting components. These systems feature complex interactions between semi-autonomous modules. Outcomes emerge from collaborative computational processes rather than individual actions. Traditional criminal law struggles with collective action beyond conspiracy and abetment. The Bharatiya Nyaya Sanhita lacks provisions addressing this distributed agency. The gap requires legislative or judicial innovation.[56]

VI. CURRENT LEGAL FRAMEWORK IN INDIA

India's legal framework addressing artificial intelligence systems remains fragmented and underdeveloped. The country lacks dedicated legislation specifically targeting AI criminal liability. Current approaches cobble together provisions from various legal domains. These include criminal statutes, information technology laws, and sectoral regulations. This patchwork approach creates significant gaps and uncertainties for courts, developers, and victims.[57]

The Bharatiya Nyaya Sanhita, 2023 serves as India's primary criminal law statute. It replaces the colonial-era Indian Penal Code without substantial modernization for technological challenges. The Sanhita maintains traditional criminal liability concepts centered on human agency. Section 2 defines fundamental concepts like "act," "omission," and "intention" in distinctly human terms. These anthropocentric definitions create conceptual barriers to AI liability. The definition of "person" under Section 2(26) potentially includes corporations but not algorithmic entities.[58]

[55] Matthew U. Scherer, Regulating Artificial Intelligence Systems: Risks, Challenges, Competencies, and Strategies, 29 HARV. J.L. & TECH. 353, 362-366 (2016).
[56] Jatin Ramaiya, Criminal Law & Artificial Intelligence: An Indian Perspective, 5 INT'L J. OF LEGAL DEVELOPMENTS & ALLIED ISSUES 7, 14-18 (2019).
[57] Anupam Chander, The Racist Algorithm?, 115 MICH. L. REV. 1023, 1034-38 (2017).
[58] Bharatiya Nyaya Sanhita, 2023, § 2, No. 45, Acts of Parliament, 2023 (India).

Section 3(5) of the Sanhita offers one potentially relevant provision for AI contexts. It extends jurisdiction to offenses committed outside India targeting computer resources within India. This could potentially address harmful AI operations conducted from foreign jurisdictions. Yet the provision assumes traditional criminal liability elements. It fails to account for AI's distinctive operational characteristics. Extraterritorial enforcement mechanisms also remain underdeveloped. This creates practical implementation challenges despite theoretical coverage.[59]

The Information Technology Act, 2000 provides another potential legal avenue. Section 43 imposes civil liability for unauthorized computer resource access or damage. Section 66 criminalizes these same acts when performed dishonestly or fraudulently. These provisions might address malicious AI deployments causing computer system damage. However, they focus narrowly on system intrusion rather than algorithmic decision harms. They fail to address AI systems operating as authorized but causing unintended harmful outcomes.[60]

Section 43A of the IT Act introduces negligence concepts relevant to AI contexts. It holds bodies corporate liable for failing to implement reasonable security practices. This provision potentially addresses negligent AI security implementations leading to data breaches. Yet it applies narrowly to sensitive personal data protection. It fails to address broader algorithmic decision harms. The compensation mechanism also operates primarily through adjudication. This creates procedural barriers to effective remedy.[61]

The Reasonable Security Practices Rules, 2011 under the IT Act provide additional guidance. These rules establish standards for protecting personal information in computerized environments. They might indirectly address certain AI security implementations. However, they focus primarily on data security rather than algorithmic

[59] Bharatiya Nyaya Sanhita, 2023, § 3(5), No. 45, Acts of Parliament, 2023 (India).
[60] Information Technology Act, 2000, § 43, § 66, No. 21, Acts of Parliament, 2000 (India).
[61] Information Technology Act, 2000, § 43A, No. 21, Acts of Parliament, 2000 (India).

decision quality. They provide minimal guidance for AI-specific risks beyond data protection. This limited scope fails to address the broader spectrum of AI-related harms.[62]

India's personal data protection framework underwent significant revision with the Digital Personal Data Protection Act, 2023. This legislation establishes comprehensive data protection principles. These principles potentially impact AI systems processing personal data. The law requires purpose limitation, data minimization, and quality requirements. These provisions might indirectly constrain harmful AI applications using personal data. However, they address data inputs rather than algorithmic processes or outputs.[63]

The Consumer Protection Act, 2019 offers another potential avenue for certain AI harms. It establishes product liability for goods or services causing harm through defects. Section 2(34) defines "product liability" broadly including design and information defects. This might encompass defective AI products causing consumer harm. Yet the Act focuses primarily on conventional consumer relationships. It poorly accommodates the complex multi-stakeholder ecosystems surrounding AI development.[64]

India's corporate criminal liability jurisprudence provides potential frameworks for AI accountability. The Supreme Court in Standard Chartered Bank v. Directorate of Enforcement established vicarious corporate liability principles. The Court held that corporations can be criminally liable for employee conduct. This doctrine potentially extends to AI systems deployed by corporate entities. However, the Court emphasized attribution through human actors within the corporation. This approach struggles with autonomous AI decisions exceeding human oversight.[65]

Sectoral regulations provide targeted approaches in specific domains. The Reserve Bank of India has issued guidelines for AI use in financial services. The Digital Health Mission

[62] Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011, Gazette of India, pt. II sec. 3(i) (Apr. 11, 2011).
[63] Digital Personal Data Protection Act, 2023, No. 22, Acts of Parliament, 2023 (India).
[64] Consumer Protection Act, 2019, § 2(34), No. 35, Acts of Parliament, 2019 (India).
[65] Standard Chartered Bank v. Directorate of Enforcement, (2005) 4 SCC 530.

guidelines address AI applications in healthcare contexts. These domain-specific approaches recognize contextual risk variations across sectors. However, they create regulatory fragmentation without overarching principles. Inconsistent approaches across sectors potentially create compliance challenges and protection gaps.[66]

Constitutional law principles potentially constrain harmful AI applications. Article 21 guarantees the right to life and personal liberty. The Supreme Court has interpreted this broadly to include privacy rights. In Justice K.S. Puttaswamy v. Union of India, the Court recognized privacy as a fundamental right. This constitutional protection potentially limits intrusive AI surveillance or profiling. However, constitutional remedies typically target state actions rather than private AI deployments.[67]

Tort law offers potential civil remedies for AI-caused harms. Negligence doctrine potentially addresses careless AI development or deployment. The Delhi High Court in The Oriental Insurance Company v. Jasdeep Singh endorsed the res ipsa loquitur doctrine. This allows circumstantial inference of negligence in certain cases. The doctrine might apply where AI systems cause harm through obviously defective operation. However, tort remedies operate primarily through civil rather than criminal liability.[68]

Intellectual property frameworks establish additional constraints on AI development. Patent law incentivizes innovation while requiring public disclosure of techniques. Copyright protection covers original AI code and potentially certain training datasets. Trade secret protection safeguards proprietary algorithms and business methods. These regimes balance innovation incentives against transparency requirements. However, they primarily address ownership rather than accountability for harmful operations.[69]

Administrative regulations increasingly target specific AI applications. The Ministry of Electronics and Information Technology released National Strategy for Artificial Intelligence in 2018. The NITI Aayog published Approach Document for India Part 1 in

[66] Reserve Bank of India, Circular on Application of Analytics in BFSI, RBI/2023-24/53 (2023).
[67] Justice K.S. Puttaswamy v. Union of India, (2017) 10 SCC 1.
[68] The Oriental Insurance Company Ltd. v. Jasdeep Singh, 2016 SCC OnLine Del 3550.
[69] Patents Act, 1970, No. 39, Acts of Parliament, 1970 (India).

2021. These policy documents articulate governance visions without establishing enforceable standards. They recognize ethical considerations while lacking binding legal force. This creates a guidance-enforcement gap in Indian AI governance.[70]

Indian courts have demonstrated limited engagement with AI criminal liability questions. The Delhi High Court in Christian Louboutin SAS v. Nakul Bajaj addressed online platform liability. The Court distinguished between active and passive intermediaries in determining responsibility. This distinction potentially applies to AI systems with varying autonomy levels. However, Indian jurisprudence lacks cases directly addressing algorithmic criminal liability. This creates significant uncertainty for courts encountering novel AI crime cases.[71]

The Telecommunication Act, 2023 potentially impacts AI systems operating through networked infrastructure. It establishes authorization requirements for operating telecommunication services. The Act broadly defines these services to potentially include certain AI applications. This regulatory framework emphasizes security and operational standards. However, it focuses primarily on communication infrastructure rather than computational decision-making.[72]

Draft legislation potentially signals future regulatory directions. The proposed Digital India Act would potentially replace the IT Act with modernized provisions. Early reports suggest enhanced algorithmic accountability provisions. The draft National E-commerce Policy proposes algorithmic transparency requirements. These initiatives suggest growing regulatory attention to AI governance. However, they remain prospective rather than current legal frameworks.[73]

[70] NITI Aayog, RESPONSIBLE AI #AIFORALL: APPROACH DOCUMENT FOR INDIA PART 1, 12-18 (2021).
[71] Christian Louboutin SAS v. Nakul Bajaj, 253 (2018) DLT 728.
[72] Telecommunication Act, 2023, No. 30, Acts of Parliament, 2023 (India).
[73] Ministry of Electronics & Information Technology, DIGITAL INDIA ACT CONSULTATION PAPER (2023).

Various ministries have established sectoral ethical guidelines for AI development. The Ministry of Health and Family Welfare published guidelines for AI in healthcare. The Ministry of Education issued guidelines for AI in education. These ethical frameworks emphasize rights protection and human oversight. However, they operate primarily through professional norms rather than legal enforcement. This creates a soft governance approach with limited deterrent effect.[74]

VII. COMPARATIVE REGULATORY APPROACHES

Global approaches to AI regulation demonstrate diverse strategies for addressing criminal accountability challenges. Different jurisdictions have developed varying frameworks balancing innovation with public protection. These comparative approaches offer valuable insights for Indian legal development. Examining international models reveals potential pathways for addressing AI accountability gaps. Each framework reflects distinctive cultural, legal and technological contexts.[75]

The European Union has pioneered a comprehensive risk-based regulatory framework. The EU Artificial Intelligence Act represents the world's first horizontal AI regulation. It classifies AI systems into risk tiers with corresponding obligations for each level. Unacceptable risk systems face outright prohibition. High-risk systems require conformity assessments, human oversight and transparency. This tiered approach links regulatory burdens directly to potential harm. Criminal enforcement mechanisms include substantial fines and potential criminal penalties.[76]

The EU framework establishes clear traceability requirements for high-risk AI systems. Documentation must identify developers responsible for compliance. The regulation mandates risk assessment throughout development and deployment lifecycles. These provisions aim to clarify responsibility chains for potential criminal liability. The Act

[74] Ministry of Health and Family Welfare, NATIONAL DIGITAL HEALTH BLUEPRINT, 42-48 (2019).
[75] Urs Gasser, AI in the Administrative State: Leveraging Diverse Disciplines for Lawmaking and Enforcement, 2019 MICH. ST. L. REV. 905, 918-922 (2019).
[76] Regulation on a European Approach for Artificial Intelligence, COM (2021) 206 final (Apr. 21, 2021).

establishes both organizational and individual accountability mechanisms. This approach directly addresses causation challenges identified in previous sections.[77]

Article 6 of the European Convention on Human Rights influences EU approaches. It guarantees procedural rights in criminal proceedings including explanation rights. The European Court of Human Rights in Tolstoy Miloslavsky v. United Kingdom emphasized predictability in criminal prohibitions. This jurisprudence influences explainability requirements in EU AI regulation. The framework emphasizes human understanding of algorithmic decisions with potential criminal consequences. This addresses AI opacity concerns in accountability determinations.[78]

The United States has developed a sectoral approach focusing on high-risk domains. The National AI Initiative Act established coordination mechanisms across federal agencies. Rather than comprehensive legislation, the US relies on domain-specific rules. Financial algorithms face accountability through SEC regulations. Healthcare AI encounters FDA oversight mechanisms. This sectoral strategy allows tailored approaches to distinctive contexts. Criminal enforcement varies across regulatory domains.[79]

The Algorithmic Accountability Act introduced in Congress proposes impact assessment requirements. Companies would evaluate automated systems for accuracy, fairness and privacy impacts. This legislation would establish documentation standards supporting criminal investigations. The proposed framework emphasizes corporate responsibility for algorithmic outcomes. This approach addresses attribution challenges through organizational accountability. The bill represents an emerging consensus on procedural accountability.[80]

US courts have addressed algorithmic evidence standards in criminal contexts. In State v. Loomis, the Wisconsin Supreme Court considered algorithmic risk assessments. The court required caution when using algorithms lacking transparency. This judicial

[77] Id. at art. 11-13.
[78] Tolstoy Miloslavsky v. United Kingdom, App. No. 18139/91, 20 Eur. H.R. Rep. 442 (1995).
[79] National AI Initiative Act of 2020, Pub. L. No. 116-283, div. E, title LVII, § 5701.
[80] Algorithmic Accountability Act, H.R. 6580, 117th Cong. (2022).

 (ISSN: 2583-7753)

approach emphasizes due process limitations on algorithmic opacity. These standards potentially extend to AI criminal liability determinations. They establish evidentiary frameworks for algorithmic culpability assessments.[81]

The United Kingdom has developed a principles-based regulatory approach. The UK AI Strategy emphasizes proportionate governance supporting innovation. The National AI Strategy prioritizes governance principles over prescriptive regulations. These principles include transparency, fairness and accountable design. Regulatory enforcement occurs through existing sectoral authorities. Criminal liability typically attaches through existing statutes rather than AI-specific provisions.[82]

The UK Alan Turing Institute has developed influential assessment frameworks. These include Algorithmic Impact Assessments and regulatory inspection protocols. The frameworks emphasize human accountability for algorithmic systems. They integrate ethics and compliance considerations throughout development lifecycles. The UK approach balances flexibility with accountability through soft governance. This creates adaptable approaches to rapidly evolving technologies.[83]

Singapore has pioneered a hybrid regulatory model combining self-regulation with government oversight. The Model AI Governance Framework provides detailed implementation guidance. The Personal Data Protection Commission established explainability and transparency standards. These include human review requirements for automated decisions. The framework establishes ethical guardrails while allowing technological innovation. Criminal enforcement occurs primarily through existing fraud and negligence statutes.[84]

[81] State v. Loomis, 881 N.W.2d 749 (Wis. 2016).
[82] U.K. Dep't for Digital, Culture, Media & Sport, NATIONAL AI STRATEGY 45-53 (2021).
[83] David Leslie, THE ALAN TURING INSTITUTE, UNDERSTANDING ARTIFICIAL INTELLIGENCE ETHICS AND SAFETY 15-24 (2019).
[84] Personal Data Protection Commission of Singapore, MODEL AI GOVERNANCE FRAMEWORK 12-18 (2d ed. 2020).

Singapore's framework emphasizes practical governance tools for AI accountability. The Implementation and Self-Assessment Guide provides detailed compliance checklists. These tools help organizations document decision-making processes. Such documentation potentially supports criminal investigations into harmful AI outcomes. The approach combines voluntary standards with regulatory consequences. This creates flexible governance without sacrificing accountability.[85]

Australia has developed a principles-based approach emphasizing human responsibility. The AI Ethics Framework establishes eight core principles including accountability. The approach emphasizes human agency as central to AI accountability. The Ethics Framework connects to existing privacy and consumer protection enforcement. The framework assigns responsibility to humans involved in AI development. This approach directly addresses attribution challenges in criminal contexts.[86]

China has implemented stringent algorithmic regulation through recent legislation. The Algorithmic Recommendation Management Provisions establish criminal penalties for harmful algorithms. The law explicitly mandates human review of algorithmic decisions. It establishes joint liability between platform operators and algorithm developers. This approach directly addresses distributed responsibility concerns. The framework creates clear lines of criminal accountability.[87]

Japan's Society 5.0 initiative establishes governance through certification systems. The approach emphasizes quality standards and professional responsibility. The Social Principles of Human-centric AI establish ethical frameworks with legal implications. These principles emphasize accountability through professional standards. The

[85] Personal Data Protection Commission of Singapore, IMPLEMENTATION AND SELF-ASSESSMENT GUIDE FOR ORGANIZATIONS 7-15 (2020).
[86] Australian Government, AUSTRALIA'S AI ETHICS FRAMEWORK 3-9 (2019).
[87] Cyberspace Administration of China, Internet Information Service Algorithmic Recommendation Management Provisions (2022).

certification model potentially addresses quality control in criminal liability contexts. It establishes clear standards against which negligence might be measured.[88]

International organizations have developed influential soft governance frameworks. The OECD AI Principles establish standards adopted by numerous countries. The UNESCO Recommendation on AI Ethics provides governance guidelines. The IEEE Global Initiative on Ethics offers technical standards supporting accountability. These frameworks establish emerging global consensus on AI governance. They potentially influence judicial interpretation of existing criminal statutes.[89]

VIII. CONCLUSION

Criminal accountability for artificial intelligence demands fundamental reconsideration of traditional legal paradigms. The mens rea and actus reus pillars face unprecedented challenges with autonomous systems. Indian criminal law must evolve beyond its human-centric foundations. The Bharatiya Nyaya Sanhita, 2023 inadequately addresses algorithmic accountability challenges. A comprehensive regulatory framework specifically targeting AI remains essential.[90]

The mens rea challenge remains particularly formidable in AI criminal contexts. Artificial intelligence systems operate without human-like consciousness or moral awareness. Their decision processes fundamentally differ from human cognitive patterns. Attributing intent, knowledge or recklessness to algorithmic systems creates conceptual inconsistencies. The Indian criminal framework must develop functional equivalents for algorithmic mental states. These equivalents should recognize AI's distinctive operational characteristics.[91]

[88] Cabinet Office of Japan, SOCIAL PRINCIPLES OF HUMAN-CENTRIC AI 8-12 (2019).
[89] Organization for Economic Cooperation and Development, RECOMMENDATION OF THE COUNCIL ON ARTIFICIAL INTELLIGENCE, OECD/LEGAL/0449 (2019).
[90] Matthew U. Scherer, Regulating Artificial Intelligence Systems: Risks, Challenges, Competencies, and Strategies, 29 HARV. J.L. & TECH. 353, 362-366 (2016).
[91] Gabriel Hallevy, THE CRIMINAL LIABILITY OF ARTIFICIAL INTELLIGENCE ENTITIES - FROM SCIENCE FICTION TO LEGAL SOCIAL CONTROL, 4 AKRON INTELL. PROP. J. 171, 175-179 (2010).

 (ISSN: 2583-7753)

The actus reus element similarly requires reconceptualization for AI applications. Identifying discrete "acts" within continuous computational processes proves problematic. The distributed nature of AI decision-making complicates traditional act identification. Causation challenges arise through complex chains involving numerous human and computational actors. India must develop causation frameworks accommodating these distributed responsibility networks. The frameworks should clarify attribution across development and deployment phases.[92]

Corporate criminal liability offers one promising avenue for addressing AI harms. Organizations deploying harmful AI systems could face criminal sanctions for inadequate oversight. The Supreme Court in Standard Chartered Bank v. Directorate of Enforcement established principles for corporate criminal liability. These principles could extend to organizational responsibility for AI deployments. This approach sidesteps the challenges of direct AI personhood while ensuring accountability.[93]

Preventative mechanisms merit equal attention alongside reactive criminal sanctions. Impact assessments, certification requirements and industry standards could prevent harms proactively. Self-regulatory frameworks with regulatory oversight show particular promise. Singapore's hybrid approach illustrates this balanced regulatory strategy. India should implement similar preventative governance frameworks. These approaches address problems before harms materialize.[94]

Sectoral approaches recognize the distinctive challenges across different AI domains. Financial algorithms present different risks than healthcare applications. Transportation AI raises issues distinct from content moderation systems. Domain-specific regulatory frameworks acknowledge these contextual variations. The United States' sectoral strategy

[92] Ryan Calo, Robotics and the Lessons of Cyberlaw, 103 CALIF. L. REV. 513, 538-545 (2015).
[93] Standard Chartered Bank v. Directorate of Enforcement, (2005) 4 SCC 530.
[94] Personal Data Protection Commission of Singapore, MODEL AI GOVERNANCE FRAMEWORK 12-18 (2d ed. 2020).

illustrates this tailored approach. India should develop similarly differentiated frameworks across key sectors.[95]

The evolving nature of AI technology demands regulatory flexibility and adaptivity. Static regulations quickly become obsolete with rapid technological advancement. Principle-based approaches maintain relevance longer than prescriptive technical standards. These frameworks should emphasize outcomes rather than specific technical implementations. Australia's principles-based strategy demonstrates this adaptive approach. Indian regulation should similarly prioritize flexible governance.[96]

IX. BIBILOGRAPHY

- **Legislation and Regulations:**

1. Algorithmic Accountability Act, H.R. 6580, 117th Cong. (2022).
2. Bharatiya Nyaya Sanhita, 2023, No. 45, Acts of Parliament, 2023 (India).
3. Commission Regulation 2021/0106 of 21 April 2021 Laying Down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act). O.J. (L 106).
4. Consumer Protection Act, 2019, No. 35, Acts of Parliament, 2019 (India).
5. Digital Personal Data Protection Act, 2023, No. 22, Acts of Parliament, 2023 (India).
6. Indian Penal Code, 1860, No. 45, Acts of Parliament, 1860 (India).
7. Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011, Gazette of India, pt. II sec. 3(i) (Apr. 11, 2011).
8. Information Technology Act, 2000, No. 21, Acts of Parliament, 2000 (India).
9. National AI Initiative Act of 2020, Pub. L. No. 116-283, div. E, title LVII, § 5701.

[95] National AI Initiative Act of 2020, Pub. L. No. 116-283, div. E, title LVII, § 5701.
[96] Australian Government, AUSTRALIA'S AI ETHICS FRAMEWORK 3-9 (2019).

10. Patents Act, 1970, No. 39, Acts of Parliament, 1970 (India).
11. Regulation on a European Approach for Artificial Intelligence. COM (2021) 206 Final (Apr. 21, 2021).
12. Telecommunication Act, 2023, No. 30, Acts of Parliament, 2023 (India).

- **Case Law:**

1. Christian Louboutin SAS v. Nakul Bajaj. 253 (2018) DLT 728.
2. Iridium India Telecom Ltd. v. Motorola Inc. (2011) 1 SCC 74.
3. Justice K.S. Puttaswamy v. Union of India. (2017) 10 SCC 1.
4. Nidhi Kaim v. State of M.P. (2017) 4 SCC 1.
5. P.S.R. Sadhanantham v. Arunachalam. (1980) 3 SCC 141.
6. Standard Chartered Bank v. Directorate of Enforcement. (2005) 4 SCC 530.
7. State of Maharashtra v. Mohd. Yakub. (1980) 3 SCC 57.
8. State v. Krishna Pillai. 1978 CrLJ 701 (Kant.).
9. State v. Loomis. 881 N.W.2d 749 (Wis. 2016).
10. The Oriental Insurance Company Ltd. v. Jasdeep Singh. 2016 SCC OnLine Del 3550.
11. Tolstoy Miloslavsky v. United Kingdom, App. No. 18139/91, 20 Eur. H.R. Rep. 442 (1995).

- **Governmental Reports and Policy Documents:**

1. Australian Government. Australia's AI Ethics Framework. 2019.
2. Cabinet Office of Japan. Social Principles of Human-Centric AI. 2019.
3. Cyberspace Administration of China. Internet Information Service Algorithmic Recommendation Management Provisions. 2022.
4. EUROPOL. Facing the Realities of AI in Criminal Investigations. 2022.

5. Malimath, V. S. Committee on Reforms of Criminal Justice System, Government of India, 2003.
6. Ministry of Electronics & Information Technology. Digital India Act Consultation
7. Reserve Bank of India. Circular on Application of Analytics in BFSI, RBI/2023-24/53. 2023.
8. U.K. Department for Digital, Culture, Media & Sport. National AI Strategy. 2021.
9. U.K. Financial Conduct Authority. Regulatory Sandboxes: Findings from the FCA Sandbox. 2019.

- **Books:**

1. Gaur, K. D. Criminal Law: Cases and Materials. 8th ed., LexisNexis, 2020.
2. Hallevy, Gabriel. When Robots Kill: Artificial Intelligence under Criminal Law. Northeastern University Press, 2013.
3. Menski, Werner F. Hindu Law: Beyond Tradition and Modernity. Oxford University Press, 2003.
4. Robinson, Paul H. Distributive Principles of Criminal Law: Who Should Be Punished How Much? Oxford University Press, 2008.
5. Russell, Stuart J., and Peter Norvig. Artificial Intelligence: A Modern Approach. 4th ed., Pearson, 2020.
6. Simester, A. P., and G. R. Sullivan. Criminal Law: Theory and Doctrine. 7th ed., Hart Publishing, 2019.
7. Williams, Glanville Llewelyn. Criminal Law: The General Part. 2nd ed., Stevens & Sons, 1961.

- **Journal Articles and Research Papers:**

1. Abbot, Ryan. "The Reasonable Computer: Disrupting the Paradigm of Tort Liability." George Washington Law Review, vol. 86, no. 1, 2018, pp. 1-45.
2. Balkin, Jack M. "The Path of Robotics Law." California Law Review Circuit, vol. 6, June 2015, pp. 45-60.
3. Calo, Ryan. "Robotics and the Lessons of Cyberlaw." California Law Review, vol. 103, no. 3, June 2015, pp. 513-63.
4. Leslie, David. Understanding Artificial Intelligence Ethics and Safety. The Alan Turing Institute, 2019.
5. Ramaiya, Jatin. "Criminal Law & Artificial Intelligence: An Indian Perspective." International Journal of Legal Developments & Allied Issues, vol. 5, no. 2, 2019, pp. 7-23.
6. Scherer, Matthew U. "Regulating Artificial Intelligence Systems: Risks, Challenges, Competencies, and Strategies." Harvard Journal of Law & Technology, vol. 29, no. 2, 2016, p. 353.
7. Vladeck, David C. "Machines Without Principals: Liability Rules and Artificial Intelligence." Washington Law Review, vol. 89, no. 1, 2014, pp. 117-50.