Journal of International Commercial Law and Technology
Print ISSN: 1901-8401

Website: https://www.jiclt.com/

Article

Governing the Algorithmic Road: Criminal Liability, Intellectual Property, and Regulatory Reform for Autonomous Vehicles in India

Article History:

Name of Author:
Mohit Mathur[1*], Dr. Aseem Chandra Paliwal[2]

Affiliation:
[1]Assistant Professor, United World School of Law, Karnavati University, Gandhinagar, Gujarat-India
[2]Associate Professor, United World School of Law, Karnavati University, Gandhinagar, Gujarat-India

Corresponding Author:
Mohit Mathur

How to cite this article:
M Mathur, A C Paliwal,: Governing the Algorithmic Road: Criminal Liability, Intellectual Property, and Regulatory Reform for Autonomous Vehicles in India, 2026:07 (1): 1138-1148

Received: *01-03-2026*
Revised: *10-03-2026*
Accepted: *26-03-2026*
Published: *28-03-2026*

Abstract: Autonomous vehicles (AVs) are rapidly transitioning from speculative technology to commercial deployment, yet most legal systems India foremost among them remain wholly unprepared to govern them. This article interrogates three interrelated domains in which that unpreparedness is most acute criminal liability attribution when autonomous systems cause death or injury intellectual property (IP) protection for the AI-driven, data-intensive innovations underpinning AV technology and the regulatory architecture India requires to enable safe, equitable, and commercially predictable deployment. Drawing on comprehensive doctrinal analysis of Indian law and systematic comparison of frameworks in the United Kingdom, Germany, the European Union, the United States, China, and Japan, the article argues that India's current legal landscape is structurally incapable of accommodating autonomous vehicles without comprehensive reform. The Motor Vehicles Act 1988 presupposes human drivers throughout. The criminal law tradition demands human mens rea that algorithms cannot supply. The Patents Act 1970 creates critical uncertainty around AI algorithm protection under Section 3(k). Trade secret law lacks statutory foundations. And data governance frameworks leave essential AV-specific questions unresolved. Against this diagnosis, the article develops an original doctrinal framework for distributed criminal liability across development, testing and deployment chains assesses India's IP gaps with comparative reference to more developed regimes and proposes an integrated reform agenda encompassing comprehensive AV-specific legislation, an autonomous vehicles safety authority, trade secret and patent reform, and an ethical governance commission. The analysis carries broader significance for any jurisdiction grappling with how law should respond to algorithmic agency in safety-critical public infrastructure.

Keywords: autonomous vehicles criminal liability mens rea artificial intelligence intellectual property India comparative law motor vehicle regulation algorithmic accountability data governance

INTRODUCTION

The autonomous vehicle is no longer a speculative technology. Google Waymo operates commercial robotaxi services across multiple American cities. Mercedes-Benz has received approval for Level 3 systems on German motorways. Baidu's Apollo platform carries paying passengers through designated districts in Beijing. The technology exists, is being deployed, and is causing fatalities the 2018 Tempe, Arizona death involving an Uber test vehicle being the most studied instance, though far from the only one

India has both the most urgent need for autonomous vehicle technology and some of the most significant legal gaps in its governance. The country records over 150,000 road traffic fatalities annually the highest in the world overwhelmingly attributable to human error. Autonomous vehicles, if adequately safe, could transform this public health crisis. Yet the country's legal infrastructure is conspicuously unprepared. The Motor Vehicles Act 1988, drafted when a driver was always a person gripping a wheel, provides no definition of an autonomous vehicle, no allocation of responsibility when machines are in control, and no regulatory pathway for deployment. The criminal law demands a guilty human mind that algorithms cannot supply. The intellectual property regime creates uncertainty around the AI innovations at the heart of AV technology. And no regulatory authority has the technical competence to certify that an autonomous system is safe for Indian roads.

This article addresses that deficit systematically. It examines three interlocking legal challenges that autonomous vehicles pose for India. First, how criminal liability should be attributed when an AV system causes

death or injury a question that exposes fundamental tensions between traditional criminal law doctrine and the realities of algorithmic agency. Second, how intellectual property law can and should protect the extraordinary innovations underpinning AV technology a question that tests the adequacy of Indian patent, trade secret, and data governance frameworks. Third, what regulatory architecture India must construct to permit safe, equitable, and commercially predictable AV deployment a question that requires learning from international experience while attending carefully to India's distinctive conditions.

The analysis proceeds as follows. Part II maps the technological landscape, explaining how AV systems function and where they fail in ways legally significant. Part III undertakes the criminal liability analysis, developing an original doctrinal framework of distributed culpability. Part IV surveys the IP terrain, identifying India's specific gaps. Part V conducts comparative regulatory analysis across six major jurisdictions. Part VI synthesises findings into a reform agenda. Part VII concludes.

Throughout, the analysis is attentive to India's distinctive features extraordinarily heterogeneous traffic pedestrians, cyclists, motorcycles, auto-rickshaws, animal-drawn carts and motor vehicles sharing roads without the lane discipline familiar to systems designed in the West variable infrastructure quality a professional driver population of approximately four million whose livelihoods are directly at stake and a legal system that has demonstrated genuine creativity in addressing novel technological challenges when properly prompted.

II. TECHNOLOGY, FAILURE MODES, AND THEIR LEGAL SIGNIFICANCE

A. The SAE Taxonomy and Its Doctrinal Implications

Any legally coherent analysis must begin with clarity about what is being regulated. SAE International's J3016 standard now the globally dominant taxonomy defines six levels of driving automation from Level 0 (no automation whatsoever) to Level 5 (full automation under all drivable conditions without any human input). The taxonomy is not merely technical vocabulary it has profound legal implications because it determines who bears responsibility for monitoring the driving environment, who must be capable of reassuming control, and at what point human agency is genuinely displaced by algorithmic agency.

At Levels 0 to 2, a human driver retains continuous supervisory responsibility for the dynamic driving task. The vehicle may assist adaptive cruise control, lane-keeping, emergency braking but the driver must always monitor the environment and be prepared to override. Existing Indian traffic law maps with reasonable adequacy onto these levels the human operator remains the legally accountable actor, and the Section 106 of the Bharatiya Nyaya Sanhita (BNS), 2023 (death by rash or negligent act) and the Motor Vehicles Act's traffic offences can operate without conceptual difficulty.

Level 3 introduces a qualitative rupture with profound legal significance. The Automated Driving System takes over the complete dynamic driving task within a defined Operational Design Domain (ODD) specified conditions of road type, speed range, weather, and geographic area but a "fall back-ready user" must be capable of resuming control when the system issues a takeover request. This is the level at which Germany's Road Traffic Act amendments have generated the most detailed legal response. The required handover dynamic in which a human must regain competent control of a fast-moving vehicle after a period of non-engagement raises deep human factors concerns that liability law has not yet adequately addressed anywhere.

At Level 4, no human fallback is required within the ODD. The system achieves a minimal risk condition autonomously if it cannot continue. This shifts the locus of legal responsibility decisively from the occupant to the entities that designed, validated, deployed, and maintain the system. Level 5 full automation under any drivable condition remains beyond current technical reach and should not structure legal frameworks at this stage.

Indian law has adopted no version of this taxonomy. The Motor Vehicles Act 1988, as amended in 2019, contains no definitions of automated driving system, operational design domain, fallback-ready user, or any equivalent concept. This definitional vacuum is not merely academic without statutory clarity about when a human is no longer the "driver," courts cannot determine which party bears traffic offence liability or compensation responsibility. The 2019 amendments, though progressive in other respects significantly enhanced penalties, mandatory recall provisions under Section 115, and stricter fitness requirements added nothing relevant to autonomous operation.

B. AV Architecture and Legally Significant Failure Modes

Modern AV systems integrate multiple technical subsystems whose failure modes have different legal implications. The perception layer sensors including LiDAR, radar, and cameras, processed through machine learning models identifies the environment. The prediction layer forecasts other road users' behaviours. The planning layer generates trajectories. The control layer executes commands. Failures at each layer produce legally distinct situations.

Perception failures are particularly significant because empirical research has documented that object detection algorithms exhibit systematically differential accuracy across demographic groups, performing markedly worse for pedestrians with darker skin tones, children, elderly individuals, and persons in traditional or non-Western dress. These disparities appear traceable to

inadequate diversity in training datasets rather than genuine technical impossibility, making them potentially actionable as design defects under product liability or, where deliberate or reckless, as candidates for criminal negligence analysis.

Prediction and planning failures where the system correctly perceives the environment but makes erroneous forecasts of behaviour or generates unsafe trajectories are especially challenging in Indian conditions. Traffic behaviour in Indian cities is characterised by high heterogeneity, frequent deviation from formal rules, minimal lane discipline, and the presence of road users not well represented in training datasets assembled primarily in structured Western environments. Deploying a system validated in San Francisco or Munich without rigorous validation in Indian conditions may itself constitute negligence.

Cybersecurity failures remote hijacking or sensor spoofing attacks introduce a further dimension that neither traffic law nor criminal law is currently configured to address in the AV context. An adversarial attack that causes a vehicle to misread its environment or disable safety systems is not merely a data breach it is potentially a lethal attack on public infrastructure requiring criminal law responses distinct from ordinary hacking.

The concept of Safety of the Intended Functionality (SOTIF), recognised in ISO 21448, captures a further legally relevant category system may cause harm not because they malfunction but because their intended functionality is insufficient for conditions encountered. A system that performs exactly as designed but fails to detect a child running into the road during monsoon conditions does not have a "defect" in the traditional product liability sense, yet the accident is no less real. Whether SOTIF-related accidents should attract strict manufacturer liability or require proof of negligent design is an open and consequential doctrinal question for Indian courts.

III. CRIMINAL LIABILITY: DOCTRINAL ANALYSIS AND A FRAMEWORK FOR REFORM

A. The Foundational Problem: Algorithmic Acts and Human Mens Rea

Criminal liability in Indian law, as in most common law traditions, rests on two foundational pillars actus reus (a prohibited act) and mens rea (a guilty mind). Bharatiya Nyaya Sanhita (BNS), 2023 calibrates culpability across a spectrum from intention through knowledge and recklessness to negligence, with criminal condemnation reserved for those who harbour morally blameworthy mental states. Section 100 defines culpable homicide as causing death with intention or knowledge that death is likely. Section 106 imposes liability for causing death by a rash or negligent act not amounting to culpable homicide the provision most commonly engaged in fatal vehicular accidents, where courts have interpreted "rashness" as conscious disregard of a known risk and "negligence" as failure to exercise the care a reasonably prudent person would exercise.

Both requirements pre-suppose a human mind. An algorithm has no consciousness, no awareness of risk, no capacity for rashness or negligence in any sense the law contemplates. The actus reus of an AV collision a vehicle moving at speed into a pedestrian is observable and uncontroversial. The mens rea is not. Who harboured the guilty mind?

The answer cannot be "no one," because that would create an accountability vacuum in which serious harm caused by foreseeable system failures attracts no criminal sanction, generating both injustice for victims and perverse incentives for industry. Nor can it be "the algorithm," which has no legal personality under Indian law and lacks the moral agency that grounds criminal condemnation. The Supreme Court's statement in Kurban Hussein Mohammeddin Rangwalla v State of Maharashtra (AIR 1965 SC 1616) that criminal negligence must involve "a very high degree" of culpability remains the correct standard the challenge is applying it to organisational and technical decision-making processes rather than individual physical conduct.

The answer, this article argues, lies in reconceptualising criminal liability around the human actors whose decisions made at temporally and causally upstream points during system design, training data curation, safety testing, and deployment authorisation created the conditions for algorithmic harm. This reconceptualization requires doctrinal work on mens rea, actus reus, causation, and corporate liability, each of which is addressed below.

B. Mens Rea Reconceptualised: Distributed Culpability Across the Development Chain

The critical insight is that mens rea in the AV context must be understood not as a single mental state at the moment of accident, but as distributed culpable mental states across a development, testing, and deployment chain. Several categories of actor warrant analysis.

Manufacturers and system integrators represent the primary locus of criminal exposure at the corporate level. A manufacturer that knowingly deploys a system with identified safety deficiencies where internal engineering data or testing results revealed inadequate performance in foreseeable conditions and that information was disregarded for commercial reasons exhibits the recklessness sufficient for criminal liability. The threshold should be gross negligence or recklessness the manufacturer must have known, or as a responsible person in their position should have known, that the system was unsafe for the deployment conditions. The analogy to pharmaceutical companies knowingly marketing unsafe drugs is apt the temporal and causal distance between the corporate decision and the ultimate harm does not attenuate the culpability of those who made the decision.

Software developers and algorithm designers may attract individual criminal liability where they introduce unsafe code recklessly, fail to implement safety-critical requirements despite awareness of the need, or participate in decisions to deploy systems they know to contain dangerous deficiencies. Proving individual mens rea within large collaborative engineering environments is genuinely demanding, and criminal prosecution of individual engineers should be reserved for cases where persons were in positions of genuine decision-making authority and exercised that authority recklessly not where they were junior contributors following specifications.

Fleet operators and deployers bear responsibility that is more proximate to ultimate harm. An operator who deploys a Level 4 system in conditions Indian traffic heterogeneity, monsoon weather, poor road markings that exceed its validated operational design domain, where that exceedance is known, exhibits recklessness. Similarly, operators who ignore safety alerts from the manufacturer, defer mandatory software updates, or create incentive structures that encourage users to override safety restrictions may attract criminal liability through commission or culpable omission.

Users in charge at Level 3 retain duties to respond to takeover requests. Criminal liability for a user who fails to respond because they were asleep, intoxicated, or engaged with a secondary activity is more tractable under existing doctrine, since the required mental state (conscious disregard of a duty to monitor) maps reasonably well onto existing judicial interpretations of recklessness. Cases involving user failure to respond will likely be the first AV criminal prosecutions in any jurisdiction.

C. Actus Reus and Causation in Algorithmic Accident Chains

Traditional actus reus doctrine was developed for cases where human bodily movements directly caused harm. AV accidents involve causal chains running from design decisions through programming, validation, deployment, algorithmic processing, and physical outcome. Three doctrinal tools, available within existing Indian jurisprudence, are capable of addressing this complexity.

First, omission liability. When manufacturers release AV systems, they perform affirmative acts approving deployment, certifying safety performance, making representations about capability that create duties. Criminal liability can attach when defendants breach those duties through culpable omissions failing to implement safety measures despite known risks, neglecting validation testing, omitting critical warnings about ODD limitations. The algorithm's decision causing immediate harm becomes the mechanism through which earlier human acts and omissions produce their effects.

Second, product-mediated harm analysis. Indian courts have recognised in the product liability context illustrated in State of Haryana v Santra (AIR 2000 SC 1888) and the broader absolute liability jurisprudence emanating from MC Mehta v Union of India (AIR 1987 SC 1086) that manufacturers can bear responsibility for harm caused through defective products without requiring that the manufacturer was physically present at the moment of injury. This logic extends naturally to AV systems.

Third, causation should focus on foreseeability and scope of risk rather than physical or temporal proximity. When manufacturers deploy systems knowing they underperform in conditions present at the deployment location, accidents attributable to that underperformance fall within the foreseeable scope of the risk created and causation is established. Where accidents result from genuinely unforeseeable edge cases that no reasonable validation regime could have anticipated, the causal connection to upstream decisions is more attenuated, and civil compensation rather than criminal sanction becomes the appropriate response.

D. Corporate Criminal Liability

The most practically significant dimension of criminal liability for AV accidents is corporate. Individual engineers rarely bear sole responsibility for systemic safety failures those failures reflect organisational culture, resource allocation, management priorities, and governance structures. India recognises corporate criminal liability, most explicitly through statutory provisions in financial regulatory statutes and through judicial construction in Standard Chartered Bank Directorate of Enforcement (AIR 2005 SC 2622) and Sunil Bharti Mittal v CBI (AIR 2015 SC 923). The doctrinal requirement that prosecutions identify specific individuals "in charge of and responsible for" the conduct presents challenges in large engineering organisations.

Statutory reform should address this directly. Corporations should be held criminally liable for AV accidents occurring through systemic organisational failures inadequate safety management culture, systematic under testing, suppression of internal safety concerns, commercial pressure overriding safety rectification without requiring identification of a single controlling mind. Sanctions should include fines calibrated to corporate revenues (to avoid fines that are merely priced in as operating costs), mandatory remediation programmes, market suspension, and in severe cases corporate dissolution.

The 2018 Tempe fatality involving Uber's test vehicle provides the most instructive precedent. The National Transportation Safety Board's investigation found systemic organisational failures weak hazard identification processes, inadequate safety culture, commercial pressure on testing timelines, and critically, the vehicle's own emergency braking system had been disabled for the test run. The prosecution of only the safety driver, while the organisation bore no criminal

consequences, illustrates precisely the accountability gap that AV-specific corporate criminal liability provisions must close.

E. The Evidentiary Architecture: Mandatory Event Data Recorders

The practical ability to investigate and prosecute AV-related offences depends entirely on preserved, authenticated evidence of system behaviour. Aviation's black box model mandatory flight data recorders and cockpit voice recorders, standardised formats, independent accident investigation provides the relevant analogy. Indian law should mandate the installation of event data recorders in automated vehicles, specifying minimum data elements (automation level engaged at time of incident, sensor inputs received, algorithmic processing outputs, control commands issued, takeover requests issued and responses received, system health status), minimum retention periods, standardised accessible formats, and clear protocols governing law enforcement access.

The Digital Personal Data Protection Act 2023 is relevant event data recorders capture personal data including location traces and potentially passenger biometric information. The framework must balance safety investigation imperatives against privacy rights, potentially through tiered access immediate law enforcement access to anonymised system-state data, fuller access to identified data only through judicial warrant, and independent investigation authority access subject to non-disclosure obligations.

IV. INTELLECTUAL PROPERTY: PROTECTION, GAPS, AND REFORM

A. Patent Protection and the Section 3(k) Problem

Patent law's central challenge for autonomous vehicles is the exclusion of algorithms from patentable subject matter. Section 3(k) of the Patents Act 1970 excludes "a mathematical or business method or a computer programme per se or algorithms." The qualifier "per se" creates doctrinal space for protecting computer-implemented inventions that produce a "technical effect," but the boundaries of that space remain uncertain in Indian examination practice and have not been settled by Supreme Court authority.

The difficulty is acute for AV technology because much of its most valuable innovation resides precisely in algorithms perception models identifying road users at speed prediction systems forecasting vehicle trajectories planning algorithms charting safe paths through complex traffic decision-making frameworks balancing competing safety objectives in real time. These algorithms, when embedded in vehicle hardware systems and producing concrete measurable technical effects improved pedestrian detection accuracy, reduced collision probability, enhanced response latency should in principle be patentable under the "per se" formulation. In practice, examination outcomes are inconsistent and the risk of rejection is high.

Comparative perspective illuminates the gap. The European Patent Office's Board of Appeals has developed a substantial body of jurisprudence distinguishing patentable technical inventions implemented in software from abstract mathematical methods excluded from protection, with the distinction turning on whether the invention contributes technical character beyond the normal physical interactions between the program and the computer. The USPTO has developed guidelines specifically addressing AI inventions following Alice Corp v CLS Bank International (573 US 208, 2014). The Indian Patent Office has issued no equivalent AV or AI-specific guidance, leaving applicants to navigate general examination guidelines that were not designed with machine learning innovations in mind.

Reform should proceed on two tracks. First, the Indian Patent Office should issue examination guidelines specifically addressing AI and AV innovations, providing worked examples that clarify when machine learning innovations embedded in vehicle control systems satisfy the technical effect standard. Second, legislative amendment should clarify Section 3(k) to explicitly permit protection of AI innovations producing concrete technical effects in physical systems, while maintaining exclusions for purely abstract mathematical methods.

B. The Trade Secret Deficit

Trade secret protection is, for most AV developers, commercially more significant than patents. Training methodologies, proprietary datasets curated over millions of kilometres, simulation frameworks, decision-making algorithm implementations, fleet operational data and safety performance statistics all represent competitive assets that developers prefer to protect through secrecy rather than patent disclosure, which would require teaching competitors how the inventions work.

India lacks comprehensive trade secret legislation entirely. Protection relies on a patchwork of common law breach of confidence, contractual non-disclosure obligations, and criminal breach of trust under Section 316 of the Bharatiya Nyaya

Sanhita (BNS), 2023. This patchwork provides uncertain scope (no statutory definition of what qualifies as a trade secret), inconsistent remedies across jurisdictions, no standards for what constitutes "reasonable measures to maintain secrecy," and no framework specifically addressing misappropriation as distinct from breach of contract.

This gap creates compounding problems. Engineers move between AV development companies, carrying tacit knowledge about algorithmic approaches and training data characteristics without clear statutory protection, the boundaries of what they may legitimately take with them are undefined. International partnerships require sharing technical details that may constitute trade secrets without enforceable protection, risk assessments by foreign partners increase. Regulatory safety assessments may require disclosure of information operators regard as commercially sensitive without confidentiality protections in regulatory proceedings, companies face invidious choices between regulatory compliance and competitive disadvantage.

The enactment of comprehensive trade secret legislation, aligned with the definitional framework of the EU Trade Secrets Directive (2016/943) information that is secret, has commercial value from its secrecy, and has been subject to reasonable protective measures is an urgent priority. The legislation should provide civil injunctive and damages remedies, criminal sanctions for wilful misappropriation, and procedural protections including in camera proceedings and protective orders enabling enforcement without requiring full public disclosure of the protected information.

C. Copyright, Training Data, and the Database Protection Gap

Copyright protection under the Copyright Act 1957 extends to computer programs as literary works, providing baseline protection for AV software. Three issues remain inadequately addressed. First, the scope of fair dealing exceptions is unclear regarding reverse engineering for interoperability and security research both legitimate activities that independent safety analysts need to conduct on AV systems, yet both potentially restricted by copyright. Legislative clarification is required.

Second, the training data underpinning AV machine learning systems represents the technology's most valuable input and legally its most uncertain asset. Raw sensor data lacks originality for copyright protection. Curated training datasets where data has been selected, labelled, cleaned, and organised through creative judgments may qualify as copyrightable compilations, but this protection is thin. More significantly, India lacks sui generis database rights comparable to those available in EU jurisdictions under the Database Directive (96/9/EC). The substantial investment in compiling driving datasets which for leading developers represents billions of dollars and millions of vehicle-hours receives no specific protection against extraction and reutilisation by competitors.

Third, the non-personal data governance framework is critically underdeveloped. The DPDP Act 2023 addresses personal data comprehensively but leaves non-personal data aggregated traffic patterns, anonymised sensor readings, statistical models derived from fleet operations in a governance vacuum. The 2020 Non-Personal Data Governance Framework report proposed treating certain community data as shared resources potentially subject to mandatory sharing obligations, a position that remains controversial and creates regulatory uncertainty for AV developers planning data infrastructure strategies. Legislative clarification of ownership rights, permissible uses, and sharing obligations for non-personal AV operational data is a prerequisite for rational investment.

D. Standard-Essential Patents and the Interoperability Imperative

As AV technologies increasingly depend on standardised communication protocols cellular Vehicle-to-Everything (C-V2X) for vehicle-to-vehicle and vehicle-to-infrastructure coordination standardised data formats for HD mapping common sensor interface specifications the question of standard-essential patent licensing becomes commercially and legally significant. Commitments to license on fair, reasonable, and non-discriminatory (FRAND) terms are industry's response to patent hold-up in standardised technologies, but "FRAND" remains deeply contested in application, with active litigation over royalty rates and injunction availability in European and American courts.

Indian courts and the Competition Commission of India will face FRAND (Fair, Reasonable, and Non-Discriminatory) disputes as C-V2X-enabled AV deployment expands. The UK Supreme Court's decision in Unwired Planet v Huawei

[2020] UKSC 37, establishing courts' jurisdiction to set global FRAND rates where parties cannot agree, is a potentially significant precedent. Developing coherent domestic FRAND jurisprudence drawing on comparative precedents and initiated through judicial training and scholarly engagement rather than awaited reactively would serve India's interests as both an importer and increasingly an exporter of AV technology.

V. COMPARATIVE REGULATORY ANALYSIS: LESSONS FOR INDIA

A. Germany: Statutory Rigour and Ethical Principles

Germany's response to autonomous vehicles provides the most systematically developed national model. The 2017 amendments to the Strassenverkehrsgesetz explicitly authorised Level 3 automated driving, defined corresponding driver obligations (the fallback-ready user must respond to takeover requests, but may direct their attention elsewhere while automation is engaged), mandated event data recorders with specified minimum data requirements, and established data protection protocols for recorded information. The landmark Gesetz zum autonomen Fahren (Autonomous Driving Act) 2021 extended authorisation to Level 4 vehicles in defined operational areas and introduced the "technical supervisor" a person monitoring vehicle operations remotely who bears legal responsibilities analogous to a traditional driver despite physical absence from the vehicle.

The 2017 Ethics Commission on Automated and Connected Driving produced twenty ethical rules that have influenced regulatory thinking internationally. Most significant is the prohibition on algorithmic discrimination in unavoidable accident situations, autonomous systems must not distinguish between persons on the basis of personal characteristics. Age, gender, disability, and ethnicity cannot be weighting factors. This is an ethical position that translates into a design requirement, a certification standard, and a liability marker system that demonstrably do make such distinctions are defective. India's analogous reform, discussed below, should adopt a comparable principle.
Germany's framework exemplifies several principles India should adopt: explicit automation-level taxonomy in statute clear allocation of responsibility across actors at each level mandatory event data recorders with defined data elements integration of cybersecurity and data protection obligations into vehicle authorisation and ethical governance principles that translate into technical standards. Its limitation is prescriptive specificity that may risk obsolescence as technology advances beyond the Level 3/4 framework the amendments contemplate.

B. United Kingdom: Insurance-Centred Liability and the ASDE Model

The United Kingdom pursued a structurally different approach. The Automated and Electric Vehicles Act 2018 established that when vehicles are operating in autonomous mode and accidents occur, the insurer becomes primarily liable for third-party claims a radical departure from fault-based liability that prioritises victim compensation speed and certainty. Insurers retain subrogation rights against manufacturers for design defects, preserving accountability through a different channel.

The Automated Vehicles Act 2024 developed this further by introducing the Authorised Self-Driving Entity (ASDE) concept a legal person (typically the manufacturer or major software developer) who bears ongoing regulatory accountability for the safety of a self-driving system throughout its operational life. This entity-level accountability is conceptually sophisticated rather than product-by-product approval at a point in time, the ASDE is responsible for the system as it evolves through software updates and fleet learning, and must notify the regulator of significant changes. For a technology that changes continuously post-deployment, this entity-centred model may be more appropriate than point-in-time type approval.

India should consider adopting an analogous "Authorised AV System Entity" concept that bears ongoing regulatory accountability, enabling the regulatory relationship to track the system through its operational life rather than terminating at initial certification.

C. European Union: Harmonisation, AI Governance, and the Liability Directive

The EU's approach operates through multiple instruments. UNECE Regulation 157 on Automated Lane Keeping Systems provides type approval requirements for Level 3 motorway driving. The AI Act, following its adoption, classifies autonomous vehicle control systems as high-risk AI, imposing mandatory conformity assessments, technical documentation requirements, explain ability obligations, and post-market monitoring. The proposed AI Liability Directive addresses the evidentiary challenges of algorithmic opacity, establishing rebuttable presumptions of causal link when high-risk AI systems cause harm and the defendant fails to comply with applicable requirements.

The EU's harmonisation through type approval has practical significance for India vehicles entering the Indian market from EU manufacturers will be designed to meet EU standards, creating de facto pressure for Indian standards to align or face market fragmentation and barriers to trade. India's active participation in UNECE Working Party 29 proceedings would facilitate regulatory convergence and reduce compliance costs for globally marketed vehicles a concrete, low-cost action India could take immediately.

D. United States: Federalism, Accountability Gaps, and the Uber Precedent

The United States presents the most instructive

cautionary example. Federal-state jurisdictional fragmentation produces inconsistent state-level AV frameworks, with California, Arizona, and Nevada taking different regulatory approaches. The National Highway Traffic Safety Administration has relied primarily on voluntary guidance and industry engagement rather than binding federal safety standards, creating accountability gaps that the Tempe fatality exposed dramatically. A decade of optimistic regulatory permissiveness produced deployment that outpaced safety validation.

The Tempe investigation's finding of systemic Uber safety culture failures inadequate hazard identification, insufficient training of safety drivers, commercial pressure on testing timelines, and the decision to disable the vehicle's emergency braking system illustrates the risks of allowing industry self-regulation without robust external accountability. India should treat the American experience as a clear warning against regulatory permissiveness in the name of innovation promotion.

E. China: State-Directed Deployment and Its Limitations

China's approach designated pilot cities with substantial state coordination, deep integration of AV policy with broader industrial strategy under Made in China 2025, extensive V2X infrastructure investment, and state-directed data governance demonstrates the potential of coordinated deployment to achieve scale and learn rapidly. Chinese AV developers have accumulated operational experience in complex urban environments that Western counterparts operating under more restrictive conditions have not.

However, China's extensive data localisation requirements, security assessment obligations for algorithmic systems, and government data access provisions create compliance burdens for international developers and raise data sovereignty concerns. The state-directed model also raises concerns about governance capture when the state is simultaneously regulator, investor, and principal beneficiary of successful deployment, independent safety oversight is compromised. India should learn from China's deployment scale ambitions without replicating its governance architecture. China's most transferable lesson for India is about public infrastructure investment. Level 4 deployment at scale presupposes high-quality roads, standardised signage, reliable V2X communication infrastructure, and comprehensive HD mapping. These are prerequisites for deployment, not consequences of it. India's infrastructure quality in most cities does not yet meet these prerequisites, and regulatory frameworks must account for this by restricting initial deployment to areas that do.

F. Japan: Precision, Safety Culture, and International Harmonisation

Japan amended its Road Traffic Act in 2019 and 2020 to permit Level 3 automated driving on public roads, with the duty of care shifting from the user to the manufacturer once automation is engaged within the system's ODD (Operational design domain). Japan's approach reflects a characteristic regulatory precision detailed technical specifications for automated driving functions, systematic integration with international standards (Japan is a major participant in UNECE Working Party 29), and coordination between the Ministry of Land, Infrastructure, Transport, and Tourism and the National Police Agency.

Japan's automotive industry culture of quality management informed by the Toyota Production System's emphasis on identifying and addressing failures at their source provides a useful complement to legal liability frameworks cultural incentives for safety that reduce the need for liability to provide all accountability incentives. This observation is relevant for India liability frameworks can be reinforced or undermined by industry safety cultures, and regulation of organisational safety management practices, not only of technical outputs, is appropriate.

VI. A REFORM AGENDA FOR INDIA

A. Comprehensive AV Legislation: The Legislative Foundations

India requires legislation that does not merely amend the Motor Vehicles Act at the margins but establishes a purpose-built framework for autonomous vehicle operation. A comprehensive Autonomous Vehicles Act should accomplish six foundational tasks.

First, statutory definitions autonomous vehicle automated driving system operational design domain fall back-ready user authorised AV system entity technical supervisor. These definitions must be aligned with the SAE J3016 taxonomy or an internationally recognised equivalent, ensuring interoperability with global regulatory frameworks and enabling Indian type approval to be mutually recognised.

Second, clear liability allocation across automation levels. At Level 3 the fallback-ready user retains duty to respond to takeover requests manufacturer and software developer bear responsibility for system failures within the ODD. At Level 4 the Authorised AV System Entity bears primary responsibility for all system performance within the ODD no occupant liability attaches for accidents occurring during autonomous operation within validated parameters. At all levels operators remain responsible for ensuring vehicles operate only within their validated ODD.

Third, mandatory safety validation and certification a staged authorisation process progressing from closed-environment testing through limited public road pilots to broader deployment, with demonstrated safety performance benchmarks at each stage. Certification must encompass not only hardware but software safety case documentation, cybersecurity assessment, and ODD validation. Certification must be renewable and revocable as systems evolve.

Fourth, mandatory event data recorders with standardised minimum specifications, tamper-evident design, law enforcement access protocols, and data protection provisions. Fifth, mandatory AV System Entity insurance for Level 4 and Level 5 operations, with coverage amounts calibrated to accident severity, providing first-instance victim compensation without fault requirement. Sixth, specific AV criminal offences deploying an uncertified system that causes death falsifying safety validation results deliberately concealing safety-critical defects from the regulator manipulating or disabling required safety systems.

B. The Autonomous Vehicles Regulatory Authority

No existing Indian regulatory body possesses the technical expertise, dedicated mandate, or operational capacity to govern autonomous vehicles effectively. The Ministry of Road Transport and Highways administers conventional vehicle regulation but lacks machine learning validation expertise, cybersecurity assessment capability, or experience with algorithmic accountability. Creating or formally designating and adequately resourcing an Autonomous Vehicles Regulatory Authority (AVRA) is essential.

The AVRA should perform the following functions establishing and enforcing technical safety standards conducting pre-deployment certification assessments administering the staged authorisation framework investigating AV incidents with powers to compel disclosure of technical data monitoring post-deployment safety performance through mandatory incident reporting and advising Parliament on regulatory updates as technology evolves. The Authority should be structured for technical independence, with mandatory industry consultation balanced by civil society and consumer representation. Formal information-sharing arrangements with NHTSA, DVSA, and EU type-approval bodies would accelerate capacity-building a sensible use of diplomatic capital given the common challenges

C. Intellectual Property Reform

Three IP reforms are immediate priorities. First, comprehensive trade secret legislation providing clear definitional standards, civil and criminal remedies, and procedural mechanisms protecting confidential information during litigation and regulatory proceedings. The legislation should explicitly address misappropriation by departing employees, by parties to failed negotiations, and through cyber-intrusion all specific risks in the AV sector.

Second, Indian Patent Office examination guidelines specifically addressing AI and AV innovations, providing worked examples clarifying when machine learning algorithms integrated with vehicle control hardware satisfy the technical effect standard. This can be accomplished administratively without legislative action and should be prioritised for immediate action. Third, legislative clarification of the governance framework for non-personal AV operational data ownership rights, mandatory sharing conditions for safety oversight, and restrictions on commercial exploitation. This is prerequisite to rational data infrastructure investment.

D. Ethical Governance: A National Commission on Autonomous Vehicle Ethics

Technical regulation and legal liability cannot exhaustively resolve the normative dimensions of autonomous vehicle deployment. Who should bear greater risk in unavoidable collision scenarios occupants, pedestrians, or other road users is a question of distributive ethics. Whether AV services must serve underserved rural populations represents a distributive justice choice. How perception system disparities across demographic groups should be weighed against overall safety performance involves contested equity trade-offs. These are questions requiring democratic deliberation, not only technical determination.

India should establish a National Commission on Autonomous Vehicle Ethics comprising technologists, legal scholars, ethicists, civil society representatives, and community members from areas affected by deployment. The Commission should develop ethical guidelines addressing algorithmic decision-making in unavoidable accident scenarios (drawing on but not uncritically adopting the German Ethics Commission's approach) establish fairness standards for perception system performance across demographic groups advise on equity in service distribution and provide a structured forum for ongoing democratic deliberation. Commission recommendations should inform regulatory certification standards and legislative drafting, creating a governance link between deliberative ethical inquiry and binding legal requirements.

E. Employment Transition and Social Licence

India's road transport sector employs approximately four million professional drivers truck drivers, taxi and auto-rickshaw operators, bus drivers whose livelihoods are directly threatened by large-scale AV deployment. This is simultaneously a welfare concern and a social licence concern. Deployment that generates visible displacement without corresponding support will erode the public trust that responsible AV integration requires, potentially generating political opposition that retards beneficial deployment and undermines safety oversight through regulatory capture by anti-AV interests.

India should develop a transition framework funded through deployment fees on commercial AV operators: retraining programmes for displaced drivers in adjacent sectors (logistics, fleet monitoring, vehicle maintenance, remote technical supervision) wage insurance during transition periods and early retirement support for workers for whom retraining is impractical. The funding mechanism levying fees on operators who benefit commercially from AV deployment aligns costs with beneficiaries and creates appropriate incentives.

VII. CONCLUSION

Autonomous vehicles expose a deep structural challenge for legal systems built on human agency how to allocate responsibility, protect innovation, and ensure safety when entities making consequential decisions are algorithms rather than persons. The challenge is not that legal principles are irrelevant mens rea, causation, patentability, reasonable care, accountability but that applying them requires careful doctrinal reconstruction in contexts their framers never contemplated.

India faces this challenge from a position of significant unpreparedness. The Motor Vehicles Act presupposes human drivers throughout. Criminal liability doctrine requires individual human mental states. Patent law creates uncertainty for AI algorithm protection under Section 3(k). Trade secret protection lacks statutory foundations. Data governance frameworks leave critical AV-specific questions unresolved. And no regulatory authority possesses the technical capacity to certify algorithmic safety.

The reforms proposed in this article comprehensive AV-specific legislation a distributed criminal liability framework that identifies culpable human decision-makers across the development chain mandatory event data recorders trade secret legislation and patent examination reform a dedicated autonomous vehicles safety authority an ethical governance commission and an employment transition framework constitute a coherent and urgently needed response. Individually, each addresses a specific legal gap. Collectively, they create an architecture within which autonomous vehicles can be deployed responsibly with clear accountability when systems cause harm, adequate protection for the innovations that make systems possible, democratic legitimacy through ethical governance, and social legitimacy through equitable sharing of benefits and burdens.

No jurisdiction has yet achieved a settled, comprehensive AV governance framework. India has the opportunity to learn from others' experience avoiding the American trap of regulatory permissiveness in the name of innovation emulating German definitional rigour and ethical principle adopting the UK's insurance-centred victim protection and entity-level accountability model and engaging with EU AI governance frameworks while constructing responses adapted to conditions that differ substantially from those prevailing in leading AV jurisdictions.

The deeper significance of this analysis extends beyond autonomous vehicles. As algorithmic systems make consequential decisions in healthcare, criminal justice, financial markets, and public infrastructure, the question of how law should govern artificial agency will pervade legal scholarship and practice. Autonomous vehicles provide the most developed and legally tractable instance of this question, because the relevant harms are physical, causation chains are relatively traceable, and regulatory analogies to aviation and pharmaceuticals are well-developed. The doctrinal frameworks, regulatory models, and governance principles developed here are contributions not only to Indian transportation law but to the broader project of subjecting algorithmic agency to the rule of law.

References

Legislation and Regulations

Automated and Electric Vehicles Act 2018 (United Kingdom) c 18

Automated Vehicles Act 2024 (United Kingdom) c 15

Consumer Protection Act 2019 (India) Act 35 of 2019

Copyright Act 1957 (India)

Digital Personal Data Protection Act 2023 (India) Act 22 of 2023

Gesetz zum autonomen Fahren (Germany) 2021

The 2017 Ethics Commission on Automated and Connected Driving produced twenty ethical rules that have influenced regulatory thinking internationally

Information Technology Act 2000 (India) Act 21 of 2000

Motor Vehicles Act 1988 (India) Act 59 of 1988

Motor Vehicles (Amendment) Act 2019 (India) Act 32 of 2019

Patents Act 1970 (India) Act 39 of 1970

Regulation (EU) 2024/1689 (Artificial Intelligence Act)

Strassenverkehrsgesetz (Germany) as amended 2017 and 2021

UNECE Regulation 157 on Automated Lane Keeping Systems (2021)

Cases

Alice Corp v CLS Bank International 573 US 208 (2014)

Indian Council for Enviro-Legal Action v Union of India AIR 1996 SC 1446

Indian Medical Association v VP Shantha AIR 1996 SC 550

Justice K S Puttaswamy (Retd) v Union of India (2017) 10 SCC 1

Kurban Hussein Mohammeddin Rangwalla v State of Maharashtra AIR 1965 SC 1616

M C Mehta v Union of India (Oleum Gas Leak) AIR 1987 SC 1086

National Insurance Co Ltd v Pranay Sethi (2017) 16 SCC 680

Standard Chartered Bank v Directorate of Enforcement AIR 2005 SC 2622

State of Haryana v Santra AIR 2000 SC 1888

Sunil Bharti Mittal v CBI AIR 2015 SC 923

Unwired Planet International Ltd v Huawei Technologies Co Ltd [2020] UKSC 37

Secondary Sources

Awad E and others, "The Moral Machine Experiment" (2018) 563 Nature 59

Delvaux M, "Report with Recommendations to the Commission on Civil Law Rules on Robotics" (European Parliament, 2017) 2015/2103(INL)

German Ethics Commission on Automated and Connected Driving, "Ethics of Automated and Connected Vehicular Traffic" (Federal Ministry of Transport and Digital Infrastructure, Berlin, 2017)

Lohmann M-F, "Liability Issues Concerning Self-

Driving Vehicles" (2016) 7 European Journal of Risk Regulation 335
Marchetti G, "Machine Learning and Law" (2019) 122 West Virginia Law Review 681
Ministry of Road Transport and Highways, "Road Accidents in India 2022" (Transport Research Wing, New Delhi, 2023)
National Transportation Safety Board, "Collision Between Vehicle Controlled by Developmental Automated Driving System and Pedestrian, Tempe, Arizona, March 18, 2018" Report HAR-19/03 (2019)
NITI Aayog, "National Strategy for Artificial Intelligence" (Government of India, 2018)
NITI Aayog, "Connected, Comprehensive, Clean: A Mobility Agenda for India 2030" (Government of India, 2018)
PRS Legislative Research, "Science and Technology Policy Brief: Autonomous Vehicles" (New Delhi, 2021)
Scherer M, "Regulating Artificial Intelligence Systems: Risks, Challenges, Competencies, and Strategies" (2016) 29 Harvard Journal of Law and Technology 353
SAE International, "Taxonomy and Definitions for Terms Related to Driving Automation Systems for On-Road Motor Vehicles" J3016 (Revised 2021)
Smith B W, "Automated Driving: Legislative and Regulatory Action" (Stanford Center for Internet and Society, 2012-ongoing)
Solaiman S M, "Legal Personality of Robots, Corporations, Idols and Chimpanzees: A Quest for Legitimacy" (2017) 25 Artificial Intelligence and Law 155
Surden H and Williams M-A, "Technological Opacity, Predictability, and Self-Driving Cars" (2016) 38 Cardozo Law Review 121
Vladeck D, "Machines Without Principals: Liability Rules and Artificial Intelligence" (2014) 89 Washington Law Review 117

