The Infinite
An International Peer Reviewed / Refereed Journal of Multidisciplinary Research

An Online Peer Reviewed / Refereed Journal
Special Issue (Volume 2| Issue 1) | October 2025
ISSN: 3048-9539 (Online)
Website: www.theinfinite.co.in

Liability in Autonomous Vehicles: A Legal and Ethical Framework

Dr. Santosh Kumar

B.Sc. (Maths), LL.M., NET, JRF, SRF, Ph.D. (LAW)

ARTICLE DETAILS

Research Paper

Keywords :

Autonomous Vehicles, Liability, Artificial Intelligence, Ethics, Motor Vehicles Law, India

ABSTRACT

Autonomous vehicles (AVs), often referred to as self-driving or driverless cars, represent one of the most transformative technological advancements of the twenty-first century. Their promise—enhanced road safety, reduced human error, and increased mobility efficiency—is counterbalanced by profound legal and ethical challenges, particularly in the realm of liability. Determining responsibility for harm when control shifts from human drivers to algorithms, sensors, and manufacturers introduces a paradigm shift in tort and criminal jurisprudence.

This paper examines the evolving legal and ethical frameworks governing liability in autonomous vehicles, focusing primarily on the Indian legal system while drawing comparative insights from the United States and the European Union. It evaluates how existing Indian laws—such as the Motor Vehicles Act, 1988, the Information Technology Act, 2000, and product liability principles—address or fail to address liability issues arising from automation.

The paper argues for a hybrid liability model that combines strict manufacturer responsibility, software accountability, and human oversight obligations. It also explores the ethical implications of algorithmic decision-making, including moral responsibility in unavoidable accident scenarios. The study concludes with recommendations for a comprehensive regulatory and ethical framework to ensure accountability, fairness, and innovation in India's emerging autonomous vehicle ecosystem.

1. Introduction

Autonomous vehicles (AVs) symbolize the convergence of artificial intelligence (AI), machine learning, robotics, and transportation technology. These vehicles are designed to operate with minimal or no human intervention, relying on complex sensors, cameras, radar, and algorithms to perceive their environment and make driving decisions. While AVs promise to revolutionize mobility by reducing accidents caused by human error, they simultaneously disrupt traditional legal principles of fault and liability.

In conventional road transport, liability is primarily assigned to human drivers based on negligence or statutory violations. However, when control shifts from human decision-makers to automated systems, attributing blame becomes ambiguous. If a driverless car causes a fatal collision, who is responsible—the software developer, the manufacturer, the vehicle owner, or the algorithm itself? This legal conundrum challenges the core assumptions of tort, criminal, and product liability law.

India, with its rapidly evolving transport ecosystem, stands at a critical juncture. The government's push toward electric and smart mobility through initiatives like National Electric Mobility Mission Plan (NEMMP) and Gati Shakti Mission underscores its technological ambitions. Yet, India lacks a dedicated legal or ethical framework for autonomous vehicles. The Motor Vehicles (Amendment) Act, 2019 does not explicitly address automation, and judicial discourse on AI liability remains nascent.

Globally, jurisdictions like the U.S. and EU have begun formulating policy frameworks, balancing innovation with accountability. The European Commission's AI Act and the U.S. National Highway Traffic Safety Administration (NHTSA) guidelines provide comparative insights into how liability can evolve in response to automation.

This paper aims to explore how Indian law can adapt to these challenges. It examines existing doctrines of liability, their limitations in automated contexts, and proposes an integrated legal-ethical framework grounded in constitutional values, technological neutrality, and consumer protection.

2. Understanding Autonomous Vehicles: Technology and Legal Implications

2.1 Levels of Automation

The Society of Automotive Engineers (SAE) defines six levels of driving automation (SAE J3016 standard):

- **Level 0:** No automation (full human control).
- **Level 1:** Driver assistance (adaptive cruise control).

- **Level 2:** Partial automation (lane keeping + acceleration).
- **Level 3:** Conditional automation (vehicle can perform most tasks but requires human intervention).
- **Level 4:** High automation (vehicle can operate in defined conditions without driver input).
- **Level 5:** Full automation (no human involvement at all).

Most modern vehicles operate at Levels 2–3, while experimental prototypes by Tesla, Waymo, and Mercedes-Benz are approaching Levels 4–5.

Each level of automation presents a different degree of human control, and therefore, different implications for liability. At Level 2, humans remain legally responsible; at Level 4–5, accountability shifts toward manufacturers and software developers.

2.2 Technological Infrastructure and AI Decision-Making

AVs rely on machine learning algorithms that interpret environmental data from multiple sensors (LiDAR, radar, cameras) to make driving decisions in real time. These systems are adaptive, meaning they learn from experience. However, machine learning introduces unpredictability—outcomes can deviate from programmed rules due to data errors or algorithmic biases.

This raises the question of foreseeability, a key element in negligence law. If an AI system acts unpredictably, can the manufacturer still be held liable for failing to anticipate every possible outcome? Or does liability require proof of defective design or inadequate risk mitigation?

Furthermore, ethical programming—how a vehicle chooses between two harmful outcomes—introduces moral liability distinct from legal fault.

2.3 Legal Characterization of Autonomous Systems

A central doctrinal challenge is determining the legal status of autonomous systems. Are AVs merely products subject to product liability, or do they act as semi-autonomous agents deserving separate legal recognition? Scholars debate whether AI should be treated analogously to corporate legal personality—an "electronic personhood" capable of bearing limited liability.

While this remains theoretical, its implications are profound. Assigning legal personhood could allow manufacturers to shield themselves from liability by transferring responsibility to the AI agent—raising ethical concerns of accountability dilution.

Indian law, rooted in human agency, currently does not recognize AI systems as legal persons. Hence, liability must be attributed to human entities—designers, programmers, or operators—within the existing legal framework.

3. Legal Framework and Liability in India

3.1 Current Legal Regime: Motor Vehicles Act and Its Gaps

The Motor Vehicles Act, 1988, as amended in 2019, remains the principal statute governing road transport. Its provisions presume human control, defining "driver" and "fault" in anthropocentric terms. Sections 134–140 deal with liability for accidents, compensation, and insurance under a no-fault regime. However, these provisions cannot be easily extended to AVs, as they depend on proof of human negligence.

The Act provides no guidance on automated decision-making, algorithmic malfunction, or software defects. In an accident involving an autonomous vehicle, the traditional frameworks—negligence, strict liability, or vicarious liability—become inadequate. There is no statutory recognition of AI as an operator or of shared liability between human and machine.

3.2 Product and Manufacturer Liability

In India, product liability is governed by the Consumer Protection Act, 2019, which imposes liability on manufacturers for defects causing harm. Under Section 84, a product manufacturer is liable if the product is defective due to design flaw, manufacturing error, or failure to warn consumers of known risks.

Applied to AVs, this means manufacturers may be liable for accidents resulting from software malfunction, defective sensors, or inadequate instructions. However, the complexity of AV ecosystems—where software, hardware, and data are developed by multiple entities—creates multi-party liability chains. Determining causation becomes exceedingly difficult.

Indian courts have not yet faced an AV liability case, but jurisprudence from product defect litigation (e.g., *Hindustan Coca-Cola v. Ashok Kumar*, 2000) suggests that strict liability may apply if harm results from a defect inherent to the product, irrespective of negligence.

3.3 Vicarious and Owner Liability

Under current Indian law, vehicle owners may still bear vicarious liability for accidents involving their vehicles, even if they were not driving. For AVs, this creates inequity: owners could be held liable for actions entirely beyond their control. Hence, legislative reform must clarify that liability shifts toward the system provider or manufacturer when automation surpasses Level 3.

3.4 Cybersecurity and Data Breach Liability

Autonomous vehicles are data-driven. Breaches in cybersecurity—hacking, unauthorized access, or data manipulation—can cause catastrophic accidents. The Information Technology Act, 2000, particularly Sections 43 and 66, penalizes unauthorized access and damage to computer systems. However, these provisions focus on criminal culpability, not civil compensation. A comprehensive AV liability framework must integrate data protection and cybersecurity accountability with traffic safety norms.

4. Comparative Perspectives: The United States and the European Union

The regulatory approaches toward autonomous vehicles (AVs) in the United States and the European Union provide valuable insights into how liability frameworks are evolving in technologically advanced jurisdictions. Both have adopted multi-layered models, combining traditional tort doctrines with product liability, data protection, and ethical accountability. India can derive essential guidance from these regimes as it prepares to legislate in the area of intelligent transport.

4.1 The United States: Fault-Based and Product Liability Approach

4.1.1 Federal and State Framework

Unlike India, the U.S. does not have a single national law governing AVs. Instead, regulation is federal–state hybrid. The National Highway Traffic Safety Administration (NHTSA) sets federal safety standards, while states control licensing, registration, and liability.

The Automated Vehicles Policy Guidance (2021) by the NHTSA emphasizes voluntary safety self-assessments (VSSA), encouraging manufacturers to disclose their safety design, testing protocols, and risk management practices. The federal approach promotes innovation but leaves gaps in legal accountability.

4.1.2 Tort and Product Liability in U.S. Law

In the absence of specific AV statutes, U.S. liability for autonomous vehicles primarily arises under tort law—particularly product liability and negligence. Under the Restatement (Third) of Torts: Products Liability (1998), manufacturers are liable if a product is defectively designed, manufactured, or lacks adequate warnings.

For autonomous vehicles, potential defendants include:

- Manufacturers (design or manufacturing defects);
- Software developers (coding or algorithmic malfunction);

- Component suppliers (sensor or hardware failure);
- Vehicle owners/operators (failure to maintain or update systems).

In Nilsson v. General Motors LLC (2018), following a fatal crash involving Uber's self-driving test vehicle, the National Transportation Safety Board (NTSB) found "inadequate safety risk assessment" and insufficient driver supervision, highlighting shared liability between human operators and the manufacturer.

Similarly, Tesla Autopilot accidents in California led to litigation asserting negligence and misleading consumer marketing. These cases illustrate that liability in the U.S. is fragmented, often determined by who exercised the "last clear control" over the vehicle.

4.1.3 Strict Liability and Software Defects

Courts in the U.S. have been reluctant to impose strict liability for software errors due to the complexity and evolving nature of algorithms. Unlike mechanical defects, software bugs may not be foreseeable or reproducible. Legal scholars such as Bryant Walker Smith (2019) propose an **enterprise liability model**, where manufacturers collectively bear responsibility for system failures, ensuring consumer protection without stifling innovation.

4.1.4 Insurance and No-Fault Mechanisms

Certain U.S. states, such as Michigan and Nevada, have proposed no-fault insurance models for AVs, where insurers compensate victims irrespective of fault and later recover costs from responsible manufacturers. This system parallels India's no-fault compensation provisions under the Motor Vehicles Act, suggesting compatibility with Indian adaptation.

4.2 The European Union: A Strict and Preventive Liability Model

4.2.1 Harmonized Legal Framework

The European Union (EU) has developed a precautionary and consumer-oriented approach to AV regulation, integrating data protection, ethics, and liability. The European Commission's 2020 White Paper on Artificial Intelligence and the forthcoming EU AI Act (expected 2025) outline a risk-based classification of AI systems, including AVs as "high-risk" technologies requiring compliance with transparency, safety, and accountability obligations.

4.2.2 Product Liability Directive (85/374/EEC)

The EU's Product Liability Directive (PLD) imposes strict liability on producers for damage caused by defective products, irrespective of negligence. A product is defective when it "does not provide the safety which a person is entitled to expect." This standard easily extends to AVs where a system malfunction—software, hardware, or algorithmic—results in injury or death.

The proposed revision of the PLD (2023) explicitly includes software, AI systems, and digital updates as products. This ensures that manufacturers remain liable even for post-sale software updates and autonomous decision-making failures.

4.2.3 Data and Cybersecurity Obligations

Under the General Data Protection Regulation (GDPR), autonomous vehicles must ensure lawful processing of personal data collected through cameras and sensors. Data breaches or misuse can attract heavy penalties (up to 4% of global turnover). The GDPR's emphasis on "data protection by design and default" complements the safety-by-design principle in the AI Act, creating an integrated regulatory ecosystem for AVs.

4.2.4 Ethics and the EU's AI Liability Directive

The EU AI Liability Directive (2022 proposal) introduces a presumption of causality where a claimant shows that an AI system malfunction likely caused harm. This reduces evidentiary burdens in complex cases where algorithmic opacity makes it difficult to prove causation—a major challenge in India's future litigation landscape.

The Directive also promotes explainability and traceability, requiring companies to maintain audit logs of AI decision-making, enabling post-accident investigation.

4.2.5 Comparative Advantages of the EU Model

The EU's regulatory philosophy combines strict liability with proactive compliance. By embedding safety, transparency, and accountability into design processes, it minimizes reliance on post-incident litigation. Manufacturers are incentivized to adopt ethical AI principles, such as fairness, transparency, and human oversight, as legal obligations rather than voluntary commitments.

4.3 Comparative Observations for India

4.3.1 Legal Orientation

The U.S. model favors flexibility and innovation, relying on tort law and state regulations. The EU model emphasizes consumer protection and ethical responsibility through strict liability and comprehensive AI governance. India currently sits at the crossroads: its legal system can learn from both by adopting a hybrid framework—balancing innovation with safety and accountability.

4.3.2 Burden of Proof and Causation

In both the U.S. and EU, plaintiffs face significant challenges in proving causation in algorithmic failures due to opacity (the "black box" problem). The EU mitigates this through presumptive causality under its AI Liability Directive—a principle India could adopt by reversing the burden of proof in AV-related accidents, compelling manufacturers to demonstrate due diligence.

4.3.3 Ethical Integration

The EU explicitly links ethics to law through principles of transparency, explainability, and non-discrimination, while the U.S. leaves ethical standards largely to industry self-regulation. India, with its constitutional foundation of dignity and justice (Articles 14 and 21), can integrate ethical AI obligations directly into its statutory framework—an approach both principled and culturally coherent.

4.3.4 Institutional Oversight

Both the EU and U.S. emphasize regulatory institutions:

- The NHTSA in the U.S. oversees safety compliance.
- The European Artificial Intelligence Board will supervise AI risk management. India can establish an Autonomous Vehicle Regulatory Authority (AVRAI) under the Ministry of Road Transport and Highways to:
    - Certify AV systems;
    - Investigate accidents; and
    - Coordinate with the Bureau of Indian Standards (BIS) for safety norms.

4.3.5 Insurance and Risk Pooling

The U.K. introduced the Automated and Electric Vehicles Act (2018), requiring insurers to cover accidents caused by AVs, then seek recovery from manufacturers. This "insurer-first" model ensures victim compensation without protracted litigation. India could adopt a similar mechanism by expanding

its Motor Vehicles Insurance Fund to cover AV accidents and establishing manufacturer reimbursement provisions.

4.4 Synthesis: Lessons for India

India must adapt its regulatory philosophy to its own social and infrastructural realities. The comparative lessons suggest four guiding principles:

1. **Hybrid Liability Model:** Combine strict product liability for manufacturers with conditional user responsibility for Levels 2–3 automation.
2. **Ethical Regulation:** Mandate AI transparency and fairness audits, akin to the EU's ethical compliance norms.
3. **Proactive Oversight:** Establish a national AV regulatory authority empowered to certify, recall, and investigate autonomous vehicles.
4. **Victim-Centric Insurance:** Develop no-fault compensation schemes ensuring timely redress, followed by subrogated manufacturer claims.

The comparative analysis shows that legal adaptability, not technological sophistication alone, will determine India's success in governing AV liability. A forward-looking framework must reconcile accountability with innovation, ensuring public trust in the age of intelligent mobility.

5. Ethical and Philosophical Dimensions of Liability in Autonomous Vehicles

5.1 Introduction: Technology Meets Morality

The legal challenges of autonomous vehicles are inseparable from their ethical implications. When artificial intelligence begins to make life-and-death decisions on the road, liability transforms from a purely legal issue into a moral and philosophical question. Traditional notions of culpability—based on human intention and negligence—become inadequate when harm results from machine decisions guided by probabilistic algorithms rather than human volition.

Ethical frameworks help lawmakers and technologists navigate questions such as:

- How should an autonomous vehicle choose between two harmful outcomes?
- Can algorithms embody moral reasoning or empathy?
- Who bears moral responsibility—the programmer, the manufacturer, or society itself?

Understanding these dimensions is essential for crafting a legal framework that respects not only technological innovation but also human dignity and justice, as guaranteed by the Indian Constitution.

5.2 The Problem of Moral Agency

5.2.1 Can Machines Be Moral Agents?

A core philosophical dilemma concerns whether AI systems can possess moral agency—the ability to make ethically accountable choices. Ethical philosophers such as Luciano Floridi (2013) argue that while AI can simulate decision-making, it lacks conscious intention, which is central to moral responsibility.

Machines can process data and predict outcomes, but they cannot comprehend the moral weight of harm. Therefore, AI should be viewed as a moral patient (an object of ethical regulation) rather than a moral agent. Responsibility must remain with humans who design, deploy, and oversee these systems.

5.2.2 The Chain of Accountability

Responsibility in AVs is distributed among multiple actors:

- Developers and Programmers who design decision algorithms.
- Manufacturers and Integrators who combine hardware and software.
- Regulators who approve deployment and testing.
- Owners and Users who activate and monitor the system.

The ethical challenge is to determine which of these agents bears the primary moral responsibility when harm occurs. Legal scholars refer to this as the "problem of many hands" (Nissenbaum, 1996)—where accountability becomes diffused across complex networks, making moral attribution difficult.

5.2.3 The Role of Intent and Foreseeability

In traditional criminal law, intent (*mens rea*) and foreseeability are prerequisites for liability. In AVs, no human directly "intends" harm at the moment of impact. Yet harm is foreseeable at the design stage. Thus, corporate moral responsibility must expand to include foreseeable algorithmic outcomes. Ethical frameworks must treat failure to anticipate algorithmic risks as equivalent to moral negligence.

5.3 The "Trolley Problem" and Algorithmic Morality

5.3.1 The Classic Dilemma

The "trolley problem", proposed by Philippa Foot (1967), asks whether it is morally permissible to sacrifice one life to save many others. For AVs, this translates to algorithmic decision-making during

unavoidable collisions: should the vehicle prioritize the passenger's safety, pedestrians, or the fewest overall casualties?

For instance, if an AV must choose between colliding with a pedestrian or swerving into a wall risking the passenger's life, the algorithm must make a split-second ethical decision—a decision that may later attract legal scrutiny.

5.3.2 Programming Ethical Algorithms

AI researchers have attempted to encode moral reasoning into AV decision systems through ethical frameworks such as:

- **Utilitarianism:** Minimize total harm (maximize overall welfare).
- **Deontological Ethics:** Follow moral rules (e.g., do not intentionally harm).
- **Virtue Ethics:** Act in accordance with moral character traits.

However, algorithmic morality faces limitations. Ethical choices cannot be universally coded, as moral values vary across cultures and societies. A utilitarian algorithm that sacrifices one life to save five might align with Western ethics but clash with Indian moral traditions rooted in *ahimsa* (non-violence) and individual dignity under Article 21 of the Constitution.

5.3.3 Public Trust and Moral Legitimacy

For autonomous vehicles to gain social acceptance, their moral programming must reflect public values. Studies (Bonnefon et al., 2016) show that while people support utilitarian decisions in principle, they prefer AVs that prioritize their own safety when purchasing. This ethical paradox complicates regulation. The moral legitimacy of AVs thus depends not only on efficiency but on perceived fairness and transparency.

5.4 The Ethics of Accountability

5.4.1 From Individual to Collective Responsibility

In human-driven accidents, blame typically rests on an individual driver. In AV contexts, responsibility becomes collective. Philosophers like Peter French (1984) argue for corporate moral agency, where corporations—through their decision-making systems—bear moral responsibility analogous to individuals.

Applying this to AVs, manufacturers and software firms should be seen as moral agents in law, responsible for ethical foresight and post-incident accountability. A firm that fails to implement safety protocols or ignores bias in training data should face moral and legal consequences comparable to negligence.

5.4.2 Transparency and Explainability as Ethical Duties

Ethical governance demands explainable AI (XAI)—systems that can justify decisions in human-understandable terms. The EU's AI Act and India's proposed Digital India Act emphasize transparency and accountability. Explainability is not merely technical but moral: victims have the right to understand *why* harm occurred. In India, this right aligns with Article 14 (equality before law) and Article 21 (right to know and live with dignity).

5.5 Cultural and Constitutional Ethics in the Indian Context

5.5.1 Dignity and the Constitutional Ethic

The Indian Constitution, especially as interpreted in *K.S. Puttaswamy v. Union of India* (2017), establishes human dignity and privacy as constitutional values. Any deployment of autonomous technology must therefore respect these principles. The ethical question is not only "who is liable" but "how can liability promote dignity and justice."

AV algorithms operating in India should be ethically aligned with these constitutional mandates. Decision-making systems must avoid discrimination, ensure fairness, and protect personal data—values consistent with the Directive Principles and Fundamental Rights.

5.5.2 Social Justice and Inclusivity

India's socio-economic diversity raises additional ethical concerns. If AVs are priced or deployed in a manner accessible only to elites, they risk reinforcing social inequality. Moreover, road safety ethics must prioritize pedestrians, cyclists, and public transport users—groups more vulnerable in India's traffic ecosystem. Hence, liability frameworks must integrate social justice ethics alongside legal responsibility.

5.5.3 Accountability of the State

Ethical responsibility also extends to the state. Under Article 12, the government must ensure that AV regulation upholds public safety without infringing liberty. If the state permits unsafe or untested AV deployment, it shares constitutional liability for failing to protect citizens' rights. Ethical governance thus demands participatory policy-making, with public consultation and continuous review.

5.6 The Role of Professional Ethics and Industry Standards

5.6.1 Ethical Codes for Developers

AI engineers and vehicle manufacturers must adopt professional codes of conduct similar to medical or legal ethics. The IEEE's Global Initiative on Ethics of Autonomous and Intelligent Systems (2019) provides a blueprint emphasizing:

- Human oversight and control;
- Transparency and accountability;
- Fairness and bias prevention;
- Respect for human rights.

These principles could be adopted by Indian engineering bodies such as the Bureau of Indian Standards (BIS) and Institution of Engineers (India) to govern AV development ethically.

5.6.2 Testing and Informed Consent

Before deployment, ethical testing protocols must simulate diverse conditions—rural roads, pedestrians, weather extremes—to ensure safety beyond controlled urban environments. Informed consent of test drivers and users must be guaranteed, reflecting both legal compliance and moral duty. Failure to ensure safety testing constitutes ethical negligence, equivalent to professional malpractice.

5.7 The Ethics of Data and Privacy

Autonomous vehicles constantly collect data on passengers, surroundings, and travel patterns. This raises two ethical concerns: consent and data ownership. Passengers must know what data are collected and for what purposes. AV manufacturers have an ethical obligation to protect this information, ensuring compliance with data minimization and purpose limitation principles akin to those under the EU's GDPR.

From an Indian perspective, misuse of data violates the constitutional right to privacy (Article 21). Therefore, liability must extend beyond physical harm to informational harm—unauthorized tracking, data leaks, or surveillance by design. Ethical AI governance demands not only safety but also respect for informational autonomy.

5.8 Ethical Governance and Public Accountability

5.8.1 Transparent Decision-Making

Ethical legitimacy requires that decisions about AV deployment—licensing, road testing, and risk assessment—be transparent and participatory. Regulatory opacity breeds mistrust. Public engagement, citizen councils, and open data policies can foster societal consensus on acceptable risk and fairness.

5.8.2 Equity in Accident Compensation

Victims of AV accidents, particularly pedestrians or low-income road users, must not face barriers to justice. Ethical policy must ensure automatic compensation through insurance or manufacturer funds, irrespective of the victim's capacity to litigate. Justice should be restorative, not merely procedural.

5.9 Synthesis: Ethical Foundations of Liability

The ethical framework for AV liability rests on four foundational principles:

1. **Accountability:** Human control and oversight remain non-transferable moral duties.
2. **Transparency:** Algorithms must be auditable and explainable.
3. **Justice:** Liability should ensure fair compensation and non-discrimination.
4. **Dignity:** Every technological decision must uphold human worth and safety.

Legal frameworks may evolve, but ethics anchors them to democratic and humanitarian values. As India advances toward intelligent mobility, embedding these ethical imperatives will ensure that innovation remains in service of society, not at its expense.

6. Challenges, Policy Gaps, Recommendations, and Conclusion

6.1 Emerging Challenges in Liability and Regulation

The adoption of autonomous vehicles (AVs) in India presents unprecedented legal, ethical, and infrastructural challenges. While automation promises improved road safety and efficiency, the lack of clear liability norms creates ambiguity for consumers, manufacturers, insurers, and regulators.

6.1.1 Absence of Legal Recognition for Autonomy

The Motor Vehicles Act, 1988, presupposes human drivers. Terms such as "driver," "operator," and "owner" cannot accommodate self-driving systems. There is no statutory recognition of autonomous driving functions, machine decision-making, or AI-driven control. Consequently, existing provisions for negligence or vicarious liability become conceptually obsolete in a driverless scenario.

6.1.2 Multiplicity of Actors and Fragmented Accountability

AV ecosystems involve multiple entities—manufacturers, software developers, data suppliers, component vendors, and network providers. This multiplicity leads to fragmented accountability and diffused liability chains. Determining fault or causation in a complex event involving sensor malfunction, software bias, and data error can become technically and legally intractable.

6.1.3 Data Opacity and Algorithmic Complexity

Algorithms used in AVs are often proprietary and opaque. Victims or regulators cannot easily access decision logs to determine causation. This "black box problem" complicates evidence gathering and legal adjudication. Without mandatory disclosure norms, claimants face severe informational asymmetry vis-à-vis manufacturers.

6.1.4 Cybersecurity Threats and Hacking Liability

Cyberattacks pose grave risks to AV safety. Hackers could seize control of vehicles, manipulate navigation systems, or extract user data. The Information Technology Act, 2000, penalizes cybercrimes but does not clarify liability where a manufacturer's inadequate cybersecurity design facilitates an attack. Should responsibility lie with the hacker, the manufacturer, or the regulator who approved insecure systems? Current law is silent.

6.1.5 Insurance and Compensation Uncertainty

India's current insurance framework assumes human fault. The Motor Vehicles Insurance Fund and Third-Party Liability Insurance mechanisms lack provisions for AV-related accidents, where no human negligence may exist. Victims risk delays in compensation while disputes over fault persist between insurers and manufacturers.

6.1.6 Ethical Legitimacy and Public Trust

Beyond law, the greatest challenge is moral legitimacy. Without transparent ethical standards for AV decision-making, public trust will erode. Citizens must be confident that AVs operate within an accountable ethical and legal framework consistent with India's constitutional values of dignity, equality, and justice.

6.2 Policy and Legal Recommendations for India

To ensure safe, ethical, and legally accountable deployment of autonomous vehicles, India must establish a comprehensive legislative framework integrating tort law, product liability, data protection, and ethical AI governance. The following recommendations are proposed:

6.2.1 Enact the "Autonomous Vehicles Regulation and Liability Act"

A dedicated Autonomous Vehicles Regulation and Liability Act (AVRLA) should be introduced to provide clarity on:

- **Definitions:** Legal recognition of "autonomous driving systems," "operator," "manufacturer," and "AI decision unit."
- **Certification:** Pre-market approval by a national authority ensuring safety, data integrity, and ethical compliance.
- **Operational Conditions:** Classification of permissible automation levels (aligned with SAE J3016).
- **Liability Distribution:** Clear allocation of responsibility between driver, manufacturer, and software provider depending on automation level.
- **Mandatory Reporting:** Obligation for manufacturers to maintain "event data recorders" (EDRs) for post-crash investigation.

Such codification will bring India in step with technologically advanced jurisdictions like the EU and the U.K.

6.2.2 Hybrid Liability Model

India should adopt a **hybrid model** combining:

1. **Strict Liability for Manufacturers:** When automation exceeds Level 3, manufacturers should bear strict liability for system failures irrespective of negligence.
2. **Conditional Human Responsibility:** For Level 2–3 automation, where human supervision remains necessary, owners may share liability for failure to intervene.
3. **No-Fault Compensation:** Immediate compensation to victims via insurance funds, followed by subrogation claims by insurers against responsible parties.

This model ensures both consumer protection and innovation flexibility, balancing deterrence with fairness.

6.2.3 Mandatory Insurance and Compensation Mechanisms

The Motor Vehicles Insurance Fund should be expanded to include a special "Autonomous Vehicle Insurance Pool" managed jointly by insurers, manufacturers, and regulators. The pool should:

- Compensate victims instantly under a no-fault regime.
- Use forensic data logs to apportion responsibility later.
- Impose penalties for non-disclosure or tampering with data.

Drawing from the U.K.'s Automated and Electric Vehicles Act (2018), India can ensure compensation continuity while allowing technical investigation to proceed independently.

6.2.4 Data Transparency and Algorithmic Accountability

Manufacturers must be mandated to maintain event data recorders and disclose system logs to regulators upon request. India's forthcoming Digital India Act and Data Protection Act, 2023 should integrate specific obligations for:

- Algorithmic explainability;
- Data retention and audit trails;
- Independent forensic access for regulators and courts.

Transparency transforms algorithmic opacity into evidence-based accountability, facilitating justice in AV-related claims.

6.2.5 Establish the National Autonomous Vehicle Authority (NAVA)

A specialized regulatory body, the National Autonomous Vehicle Authority (NAVA), should be established under the Ministry of Road Transport and Highways (MoRTH) to:

- Certify AV technologies before deployment;
- Oversee real-world testing and licensing;
- Investigate accidents and maintain a public database;
- Coordinate with BIS for safety standards and data protocols.

NAVA could function similarly to the U.S. NHTSA and the European Artificial Intelligence Board, ensuring cohesive national oversight.

6.2.6 Integration of Ethical AI Guidelines

India should adopt binding ethical AI standards within AV regulation. These should align with:

- The NITI Aayog "Responsible AI for All" framework (2021);
- The IEEE Global Initiative on Ethics of Autonomous Systems (2019);
- The constitutional principles of fairness, dignity, and non-discrimination.

Manufacturers must conduct Ethical Impact Assessments (EIA) before commercialization, evaluating potential bias, harm scenarios, and cultural compatibility of algorithmic decisions.

6.2.7 Strengthen Cybersecurity and Data Protection

AVs must be designated as "critical information infrastructure" under Section 70 of the IT Act. Manufacturers should:

- Employ end-to-end encryption and secure firmware updates.
- Report cyber incidents to CERT-In (Computer Emergency Response Team).
- Maintain liability for foreseeable cybersecurity failures.

Failure to ensure cybersecurity should constitute negligence per se, attracting civil and criminal penalties.

6.2.8 Public Participation and Ethical Oversight

Legal legitimacy demands public trust. Therefore:

- AV deployment policies should be subject to public consultation;
- Ethical oversight boards with representatives from civil society, academia, and industry should monitor compliance;
- Regular transparency reports should disclose accident data, near-miss incidents, and ethical risk assessments.

Public participation transforms governance from technocratic control to democratic accountability.

6.3 Institutional and Educational Measures

Beyond legal reform, India must foster institutional capacity and ethical awareness.

6.3.1 Judicial and Administrative Training

Judges, prosecutors, and regulators must receive training in AI technologies, algorithmic forensics, and data ethics. Specialized benches could handle disputes involving AI liability, ensuring technical proficiency in adjudication.

6.3.2 Technical Standardization

The Bureau of Indian Standards (BIS) should collaborate with global bodies such as ISO and IEEE to develop technical standards for AV safety, algorithmic transparency, and interoperability. Harmonization will facilitate cross-border regulatory recognition and consumer confidence.

6.3.3 Public Awareness and Consumer Rights

Consumer education campaigns should inform the public about AV capabilities, risks, and safety responsibilities. Clear labeling—stating automation levels and limitations—should be mandatory to prevent misleading marketing practices, a recurring issue in Tesla's "Autopilot" controversies.

6.4 Ethical Governance in Practice

Law without ethics risks hollow legality. Ethical governance must be the normative foundation of AV regulation in India.

1. **Accountability over Automation:** Every algorithmic decision must remain traceable to a human or corporate entity.
2. **Transparency over Secrecy:** Openness in system design and data logs enhances trust.
3. **Justice over Expediency:** Compensation mechanisms must prioritize victims over corporate profits.
4. **Dignity over Efficiency:** The right to safety and privacy outweighs market or technological convenience.

Embedding these values within the regulatory framework transforms AV governance into an expression of constitutional morality—a principle reaffirmed in *Puttaswamy* and central to India's digital future.

7. Conclusion

Autonomous vehicles embody both technological hope and legal disruption. They promise to reduce human error—responsible for over 90% of road accidents—but simultaneously blur the boundary between human and machine responsibility. The question "who is liable?" transcends mere statutory interpretation; it encapsulates the evolving relationship between technology, morality, and constitutional law.

India's current legal infrastructure—anchored in human-centric concepts of negligence and control—cannot adequately address the distributed causality of AI-driven mobility. Comparative insights from the United States and the European Union show that no single liability model suffices; instead, hybrid

approaches combining strict product liability, ethical regulation, and proactive oversight yield the best balance between innovation and accountability.

The road ahead demands not only legal reform but a moral recalibration of accountability in the age of automation. Liability should not be viewed as punishment but as a mechanism of justice and trust, ensuring that technology serves humanity responsibly.

Ultimately, the legitimacy of autonomous vehicles in India will depend not on how fast they move but on how justly they stop—when things go wrong. Law, ethics, and technology must co-evolve to safeguard the constitutional promise that even in an age of machines, human dignity remains inviolable.

References

Barfield, W., & Pagallo, U. (Eds.). (2020). *Research handbook on the law of artificial intelligence*. Edward Elgar Publishing.

Bonnefon, J. F., Shariff, A., & Rahwan, I. (2016). The social dilemma of autonomous vehicles. *Science, 352*(6293), 1573–1576. https://doi.org/10.1126/science.aaf2654

Brownsword, R. (2019). Law, technology and society: Reimagining the regulatory environment. *Routledge*.

Bryson, J. J. (2018). Patiency is not a virtue: AI and the design of ethical systems. *Ethics and Information Technology*, *20*(1), 15–26.

European Commission. (2020). *White Paper on Artificial Intelligence: A European approach to excellence and trust.* https://ec.europa.eu

European Commission. (2023). *Proposal for a Directive on AI Liability.* https://digital-strategy.ec.europa.eu

Floridi, L. (2013). *The ethics of information.* Oxford University Press.

Goodall, N. J. (2014). Machine ethics and automated vehicles. In *Road Vehicle Automation* (pp. 93–102). Springer.

IEEE Global Initiative. (2019). *Ethically aligned design: A vision for prioritizing human well-being with autonomous systems*. IEEE.

Latonero, M. (2018). *Governing artificial intelligence: Upholding human rights & dignity*. Data & Society Research Institute.

Nilsson v. General Motors LLC, No. 18-cv-00471 (N.D. Cal. 2018).

Nissenbaum, H. (1996). Accountability in a computerized society. *Science and Engineering Ethics, 2*(1), 25–42.

Pagallo, U. (2017). The laws of robots: Crimes, contracts, and torts. *Springer International Publishing.*

Puttaswamy v. Union of India, (2017) 10 SCC 1 (India).

Restatement (Third) of Torts: Products Liability §1 (American Law Institute, 1998).

Smith, B. W. (2019). Automated driving and product liability. *Michigan State Law Review, 2019*(1), 1–35.

United Kingdom Parliament. (2018). *Automated and Electric Vehicles Act 2018.* https://www.legislation.gov.uk

United States National Highway Traffic Safety Administration (NHTSA). (2021). *Automated vehicles 4.0: Preparing for the future of transportation.*

Wachter, S., Mittelstadt, B., & Floridi, L. (2017). Transparent, explainable, and accountable AI for automated decision-making. *Science and Engineering Ethics, 23*(5), 1375–1382.

World Economic Forum. (2020). *Ethics by design: Principles for good governance of AI.* https://www.weforum.org