International Journal for Multidisciplinary Research (IJFMR)
E-ISSN: 2582-2160 ● Website: www.ijfmr.com ● Email: editor@ijfmr.com

# Legal Challenges in Establishing Negligence and Causation in AI-Based Automobile Accident

**Kashaf Ujala[1], Dr. Vinit Kumar Sharma[2]**

[1]LL.M. Student, University Institute of Legal Studies, Chandigarh University, Mohali, Punjab, India.
[2]Associate Professor, Law, University Institute of Legal Studies, Chandigarh University, Mohali, Punjab, India.

**Abstract**
Rapid deployment of artificial intelligence (AI) in driver-assistance and autonomous driving technologies is changing the character of road incidents, and therefore how legislation must view them. In the ordinary law of tort and criminal law there is a human agent whose conduct can be measured by the standard of a reasonable man, and whose actions can be linked by a chain of factual and legal causation to the harm. All of these premises are challenged when a machine-learning system perceives, predicts and makes decisions in milliseconds only. This study investigates the legal obstacles in proving negligence and causation in AI-related vehicular incidents, with a major focus on Indian legislation, but also making comparisons with the United Kingdom, Germany, the European Union and the United States. It takes a doctrinal and comparative approach to examine the duty of care, the standard of care, breaches, factual and legal causation, the apportionment of responsibility amongst drivers, manufacturers, software developers and other members of the supply chain, and the evidential challenges arising from opaque algorithms and vehicle data. The study concludes that the existing negligence framework is only partially adapted to deal with AI-related damages: the standard of care for algorithms is unclear, the "black box" hinders the demonstration of breach and causation and accountability is scattered across a fragmented supply chain. It advocates a composite approach including the legal identification of the accountable party at each automation tier, mandatory event data documentation and transparency, contestable evidentiary assumptions and an insurance-supported no-fault compensation framework, while making targeted recommendations for the reform of Indian legislation.

**Keywords:** Artificial Intelligence; Autonomous Vehicles; Negligence; Causation; Product Liability; Motor Vehicles Act; Algorithmic Accountability

## 1. INTRODUCTION

India sees a large number of civil and criminal cases resulting from road incidents. The laws governing these incidents are for a human operator, whose negligence can be established, measured and punished. That assumption now is being challenged. Sophisticated driver-assistance systems (ADAS) and possibly automated driving systems (ADS) use machine-learning algorithms to process sensor data, predict actions of other road participants and make driving decisions with little or no human intervention. SAE International defines six levels of driving automation, ranging from Level 0 (no automation) to Level 5 (full automation) [1]. The legal implications of each level relate to who is responsible for monitoring the roadway and who must take over when the system reaches its limitations. The problem is not technical

but mainly conceptual. In common law jurisdictions like India, negligence is shown by proving that there was a duty of care owed, that it was breached, and that the breach caused harm. Each component presupposes the existence of a human agent: someone to whom an obligation is owed, whose behaviour can be assessed against that of a prudent person, whose actions can be traced to the harm through a recognisable chain of events. A neural network trained on vast distances of driving data, remotely updated by its creator, and used in a car owned by one person but driven, monitored, or simply sat in by another does not fit any of these categories neatly.

This is a matter of grave legal consequence and there are actual cases that prove it. In the 2018 Tempe, Arizona incident, investigators found that the automated driving system saw the pedestrian several seconds before the collision, but inconsistently changed her classification and did not accurately predict her trajectory, while the human safety operator was visually distracted and the developer's safety risk assessment and supervision were insufficient [2]. Similarly, the investigation of the Mountain View vehicle using partial automation uncovered a convergence of system constraints, negligence of the driver and inadequate oversight of driver involvement [3]. In all cases, damage was the result of a complex of contributing factors involving a person, a machine, a corporation and a regulatory body, a situation the doctrine of negligence, looking for a single perpetrator, is ill-equipped to deal with.

This paper poses three questions. First, what do obligations of care look like when the critical actions are algorithmic? What are the benchmarks of care? And what are violations? Second, how does one determine factual and legal causation when the reasoning behind a system's decision is not easily articulated? Third, who is responsible — drivers, owners, manufacturers, software developers or others in the supply chain? What are the laws that will enable accountability in India? The examination is on the Indian legislation with comparative insights from United Kingdom, Germany, European Union and United States. Section 2 is the literature review; Section 3 is the methodology; Section 4 is the legal analysis; Section 5 is the findings and suggestions; and Section 6 is the conclusion.

## 2. LITERATURE REVIEW

Scholarship on liability for automated driving has developed along five lines.

### 2.1 Tort liability and the manufacturer

Judicial bodies and juries would find these questions of foreseeability and defects complicated by the shift of liability from operators to manufacturers of self-driving cars, as predicted by Marchant and Lindor [4]. Smith says that current product liability doctrines are mostly adaptable to automated driving, but points out outstanding issues with defects and warnings [5]. Abbott suggests that once artificial intelligence systems become superior to humans, the negligence standard should be based on the performance of a "reasonable computer" rather than a reasonable person [6].

### 2.2 Foresight, control and the limits of tort

Scherer argues that the independence and unpredictability of artificial intelligence systems stand in opposition to the principles of foreseeability and control that are the foundation of tort law and regulation [7]. Calo notes a pertinent observation on the emergent behaviour of robotic systems which can generate outcomes that are unexpected by the designer and the user [8].

### 2.3 Responsibility gaps and criminal liability

According to Matthias, the development of learning automata creates a "responsibility gap" in which no one can be fairly held responsible for the actions of a machine [9]. Hevelke and Nida-Rümelin propose that for autonomous vehicles, accountability should be shared between users and manufacturers through

insurance-type contracts [10]. Gless, Silverman, and Weigend study the applicability of criminal-law notions of fault to the damage caused by autonomous vehicles [11]. The idea of a "moral crumple zone" that Elish introduced is about how we tend to place blame on the person closest to the machine, even when that person has little power to change anything [12].

### 2.4 Opacity and causation

Burrell identifies three forms of opacity in machine learning: intentional corporate secrecy, technical lack of understanding, and the difference between algorithmic and human cognition [13]. Bathaee argues that the opaque nature of AI undermines legal assessments that depend on evidence of intent and causation [14].

### 2.5 Regulatory responses

The Law Commissions of England and Wales, and Scotland, have proposed a new legal framework for autonomous vehicles based on a responsible party in charge of the automated driving system [15]. This was largely achieved through the Automated Vehicles Act 2024 [16], which builds upon the insurer-first framework created by the Automated and Electric Vehicles Act 2018 [17]. The European Union has updated its product-liability framework to include software and to simplify evidence requirements [18], in line with its risk-oriented regulation of AI.

### 2.6 Research gap

Most of this research is related to the legal systems of the United States, the United Kingdom or Europe . There has been relatively little analysis on the applicability of Indian laws on motor accidents, consumer protection, criminal negligence and electronic evidence to an incident involving a vehicle operated by an AI. The present study examines the deficiency by dissecting each ingredient of negligence under Indian jurisprudence and testing it against the comparative frameworks.

## 3. RESEARCH METHODOLOGY

This research adopts a doctrinal (black-letter) approach, supplemented by comparative legal analysis. The doctrinal part examines basic Indian legislation, i.e. Motor Vehicles Act, 1988 [19]; Consumer Protection Act, 2019 [20]; Bharatiya Nyaya Sanhita, 2023 [21]; Bharatiya Sakshya Adhiniyam, 2023 [22]; and Digital Personal Data Protection Act, 2023 [23], along with landmark judicial decisions on negligence, res ipsa loquitur, and electronic evidence. Indian negligence law has developed in the common law tradition and hence English decisions are also used as persuasive authority.

The comparative element examines the United Kingdom, Germany, the European Union and the United States. They were selected because they illustrate distinctive regulatory approaches: priority for insurer compensation, custodian and driver responsibilities with data documentation, product liability reform, and individual tort adjudication. Official reports of accident investigations are factual representations of the distribution of failures among participants, not empirical evidence.

The analytical framework consists of the elements of negligence: duty, standard and breach; causation and remoteness; and damage. There are also two overarching concerns: the distribution of responsibility and the problem of evidence. Secondary sources include peer-reviewed scholarly articles and reports on legal reform.

The study has limitations. It does not compare hypotheses to accident data, and lacks empirical evidence. The legal and technological environment in this area is evolving rapidly and statements about foreign instruments reflect the situation at the time of writing. The author has not found any Indian appellate decision recorded which has squarely addressed the issue of liability in an accident involving an automated

driving system. Accordingly, the interpretation of Indian law is by analogy and is to be taken as a proposition and not established jurisprudence.

## 4. LEGAL ANALYSIS

### 4.1 Levels of Automation and the Allocation of Legal Roles

The starting point of the examination should be the degree of automation, since it determines who is expected to drive the vehicle. At Levels 0 to 2, the human operator is legally recognised as the driver and bears, or supervises, the entire driving responsibility. Level 3: The system operates in a defined domain but expects human intervention when asked. At Levels 4 and 5, the system performs the whole task itself. Level 4 works only in a limited domain and does not expect human involvement. The legal accountability implications are captured in Table 1.

**TABLE 1. VEHICULAR AUTOMATION AND EXPECTED LEGAL ACCOUNTABILITY**

| Level | Who monitors the road | Likely primary legal actor | Main legal difficulty |
|---|---|---|---|
| 0-2 | Human operator, persistently | Operator; producer for flawed design or insufficient alerts | Excessive dependence and self-satisfaction; sufficiency of driver oversight. |
| 3 | System, until it demands authority | Controversial: chauffeur or maker | Appropriateness of handoff period; who was accountable during the failed incident |
| 4-5 | System | Maker, innovator, or manager | Lack of human control; demonstration of a design imperfection and its causative link. |

There is no class of automated vehicle in the Motor Vehicles Act, 1988. It assumes a human driver, who has duties, such as taking reasonable steps to get medical assistance for an injured person after an accident, which a machine cannot effectively do [19]. So Indian law has no statutory response to the basic question of the identity of the "driver" while the system is driving

### 4.2 Duty of Care

The duty of care causes the human operator slight difficulties and the others major difficulties. A road users has a duty to other road users, and automation does not remove that duty at Levels 0 to 2. For producers, the neighbour principle established in Donoghue v. Stevenson clearly endorses a responsibility toward individuals who may be predictably injured by a faulty product [24]. The Caparo criteria of foreseeability, proximity, and fairness are readily satisfied for motorists, who are specifically the individuals an automated driving system aims to safeguard [25]. Harder questions involve the lower participants in the hierarchy: the vendor of perception software, the source of mapping or training data, and the organization providing over-the-air updates. Each can plausibly affect safety, but each may claim

it supplied only one part which was incorporated by another party. These obligations have not yet been assessed by the Indian judiciary, but there is no reason to exclude them: duty depends on foresight and control, and those who design and alter safety-critical software have extensive power over the vehicle's operations. There should also be a recognition of the continuing duty to monitor and update the systems put in place, in a similar way to the duty to warn.

**4.3 Standard of Care and Breach**

The first place where the doctrine really begins to falter is the standard of care. For a human operator, the standard is the skilled, competent driver. There is no one standard for an algorithm. There are 3 contenders. The first type is the reasonable human operator. This is instinctive but arguably too permissive for a system that does not get tired, drink alcohol or use a mobile phone. The second standard Abbott proposes is the "reasonable computer" standard, which evaluates the system in comparison to similar systems, or in comparison to what is technologically feasible [6]. The third concerns regulatory or technical compliance, which is reassuring, but like other technical standards, is more appropriately considered a marker of due diligence than definitive proof of it. Developers may also refer to the Bolam principle [26], which states that compliance with recognised professional standards is a defence to claims of breach, a doctrine that has been used by Indian courts in cases of professional negligence. Judicial bodies ought to be wary in adopting the practices of an emerging industry, in which safety evaluations are largely self-regulated, as the ultimate standard of reasonableness.

The breach is hard to notice because the vital decision was made by a model instead of a thinking person. The courts will likely have to decide where the human error lies in the decisions that come before the machine moves: how the perception and planning system is set up, the selection and representativeness of training data, how the system is validated and tested, the decision to allow the system on public roads, what is told to the operator about what the system can do, the adequacy of driver monitoring systems. From this point of view the fault is not in the instantaneous choice but in the evolution and implementation, in line with the Tempe conclusions regarding insufficient safety risk evaluation and operator supervision [2].

Where supervision by humans is needed, breaches must be examined in light of known human limitations. A driver told to manage a system that works reliably for long periods will become indifferent eventually. If there is a failure of automated system and the regulation holds the driver responsible for not responding immediately, the individual may become a "moral crumple zone" absorbing responsibility for deficiencies in system architecture [12].

**4.4 Causation in Fact**

Factual causation is usually established by the "but for" test [27]: would the harm have occurred but for the conduct of the defendant? An atypical counterfactual is used for the AI-induced incident examination. The plaintiff must prove that the accident could have been avoided with an alternative system, perhaps differently designed, trained or tested, or by a more attentive driver. To demonstrate this, one must reconstruct the system's perception, prediction, and planning at the pertinent time, and then prove that a viable alternative could have led to a superior result. In the case of a deep neural network, this reconstruction is impossible because the internal representation of the network is in general not understandable by a human [13], and the output may be different for slightly different inputs, which means that the counterfactual cannot be trusted to be able to re-execute the program. Bathaee argues that the Ai blackbox nature makes intent and causation hard to prove[14].

Made worse by concurrent factors. A crash could result from a sensor constraint, a software misclassification, a distracted motorist, or poor road signage. The House of Lords' willingness in Fairchild to modify the "but for" test in exceptional circumstances where scientific evidence is unavailable [28] shows that courts are able to adapt causation in the face of evidential difficulties. While this logic can be applied to AI-related incidents, it is not a proven theory in India. Distributing the blame across multiple contributors would be helpful than refusing it because there was no single attribution.

**4.5 Legal Causation, Distance and Intervening Acts**

And even when factual causation has been established, the injury must not be too remote. The Wagon Mound test asks if the type of harm was reasonably foreseeable [29]. A developer may claim that the behaviour of a learning system in a rare "edge case" was not predictable and that this emergent decision breaks the causal chain. Scherer describes this problem in general terms [7]. The more reasonable view is that collision injuries to road users are obviously foreseeable as a type of damage, and the mere assertion that the particular failure mechanism was not anticipated is inadequate. Learning systems are known to be inherently unpredictable and developers accept that risk when they deploy them on public roads.

Intervening actions consist of the behaviour of a human operator that does not take control, a malicious third party, a road authority that does not fix a danger or the actions of the pedestrian themselves. An intervening act will normally break the chain of causation only if it is unforeseeable or sufficiently independent. In the Mountain View incident, driver inattention and a malfunctioning highway attenuator, as well as system constraints, contributed [3]. If a system design assumes that the driver will not be attentive to the system due to a lack of driver engagement monitoring, then that driver inattention should lead to liability through contributory negligence, not absolve the manufacturer. The Indian judiciary has allocated composite and contributory negligence in vehicular accident claims, meaning the framework is in place.

**4.6 Accountability Distribution Under Indian Law**

There are four avenues of liability under contemporary Indian legislation and none of them have been crafted for automation. The Motor Vehicles Act is the first law and it provides for filing claims against the driver, owner and insurer, makes insurance against third party compulsory and imposes strict liability without fault in case of death and permanent disability [19]. This framework is applicable to Levels 0 to 2 because the owner's liability and the insurer's duty to cover third-party claims are not contingent on proving manufacturer fault; it provides victims with some possibility of redress even in circumstances of low technological understanding. Where the gap is that there is no specific statutory remedy for an insurer who pays out to try and get his money back from the developer or manufacturer.

The second aspect concerns product liability under the Consumer Protection Act, 2019 [20], which acknowledges claims against producers for manufacturing defects, design defects, and inadequate warnings. This is the normal way against a car maker, but the limitations are practical. Whether embedded software and over-the-air updates constitute a "product" is uncertain. A claim of design defect demands technical proof that the claimant might find challenging to present. And a pedestrian or bystander who did not purchase the vehicle might have trouble pursuing a consumer claim.

The third is common law negligence that can be used against any party.This is still a possibility but has the evidentiary burdens discussed above. In a case of accident, the Supreme Court applied the principle of res ipsa loquitur [30]. Res ipsa loquitur means the facts speak for themselves. If the accident is such that it does not take place without negligence and the object was in the dominion of the defendant, a presumption of negligence arises. In the case of automated vehicles, the responsibility for explaining

failures may lie with the party in control, but the concept of "control" remains contested when the driver and the system work together.

The fourth category is strict or absolute liability. The Supreme Court in M. C. Mehta laid down a precedent for absolute liability on the businesses in the case of inherently hazardous operations [31]. This would be controversial and unlikely to apply to self-driving cars under the present laws, but the reasoning indicates that Indian law may move away from fault where victims are unable to protect themselves from profit-driven risks.

**4.7 Legal Liability for Criminal Acts**

Under the Bharatiya Nyaya Sanhita, 2023 [21], penalties are prescribed for causing death by negligence (Section 106) and for rash or negligent driving on public roads (Section 281). The Supreme Court has held that criminal negligence requires gross negligence or recklessness and not mere lack of care [32]. Two outcomes occur. first, the supervisor of a level 2 vehicle, ignoring clear instructions, may hit that limit, and individual drivers may face prosecution while the architects of the system escape scrutiny. In the Tempe case, as widely reported, it was the human safety operator, not the developer, who faced prosecution. Second, the liability of corporations or developers is problematic: criminal law requires a guilty mind connected to an individual or the directing mind of a corporation, and errors arising from machine learning rarely correspond to any person's mind. If there is no provable recklessness, there is little remedy under the criminal law.

**4.8 Proof and Information**

The evidence is the pragmatic impediment. Data held by manufacturers and developers, such as sensor logs, model iterations, software update histories, system alerts, and driver monitoring records, is necessary to determine breach and causation. Three problems arise. First, access: the party with the largest stake in the outcome controls the information, and may resist disclosure on the grounds of trade secrets. Secondly, admissibility: electronic records require the certification as required under section 63 of the Bharatiya Sakshya Adhiniyam, 2023 [22], which continues the practice followed under the earlier Evidence Act in Anvar P. V. [33] and Arjun Panditrao Khotkar [34]. The certificate has to come from the person in charge of the device, who in this case is often the other party. Third, privacy: Automotive data could contain locational and biometric data of drivers and passengers, so its collection and dissemination should comply with the Digital Personal Data Protection Act, 2023 [23].

Without a legal requirement to record and retain data from driving-automation systems in a standardised, tamper-proof format that can be accessed by courts and investigators, important evidence could be lost, overwritten or monopolised by one party. But there is another option: Germany. The country’s Road Traffic Act requires that positional and temporal data are recorded when control is handed over from the driver to the system [35].

**4.9 Comparative Approaches.**

United Kingdom. Under the Automated and Electric Vehicles Act 2018 the insurer is liable for damage caused by an autonomous vehicle which is operating on its own [17], but there is still a possibility of recovery from other liable parties, meaning victims do not have to prove that the manufacturer was negligent. The Automated Vehicles Act 2024 [16], as recommended by the Law Commissions, establishes a authorised self driving entities that operates the vehicle, which means the user-in-charge is not liable for the driving function.

Germany. Amendments to the Road Traffic Act allow highly and fully automated operations, but the keeper remains responsible, the driver must be ready to take over when requested, and data documentation

is required [35].

European Union. The updated Product Liability Directive classifies software as a product, extends liability to component manufacturers, allows courts to order the disclosure of evidence, and provides for presumptions of defect or causation where technical complexities make it excessively difficult for the claimant to prove [18]. The AI Act [36] imposes requirements on high-risk artificial intelligence systems. United States of America: There is no federal liability scheme; claims are determined state-by-state under existing negligence and product liability laws. In 2025, a jury ruling in Florida (reported pending) attributed part of the liability for a deadly collision involving a driver assistance system to the producer [37]. The judicial bodies might take into account more factors than the operator.

These jurisdictions invariably see three approaches — identifying a responsible party (insurer, authorised entity or manufacturer), enabling evidence through data documentation, transparency and assumptions, and keeping a compensation route that is disconnected from the establishment of fault.

## 5. FINDINGS AND SUGGESTIONS

### 5.1 Findings

The Indian legislation does not cover the definition for automated driving or the responsible party. The Motor Vehicles Act presumes the presence of a human operator. A duty of care in principle applies to manufacturers and developers, but its applicability to downstream suppliers and update providers is not yet settled. The criteria for the care of an algorithm remain unclear, and any failure is more accurately located in its design, testing, implementation and notifications rather than in the instantaneous choice of the algorithm. Algorithmic opacity renders difficult the establishment of the “but for” counterfactual, so that relaxed causation and apportionment must be adopted. Responsibility is spread across a decentralised supply chain; the present no-fault and insurance systems give the quickest resolution at Levels 0 to 2 but lack a structured recourse pathway against manufacturers. Criminal law can have a “moral crumple zone” effect by holding individual drivers accountable. The main practical problem with accountability lies in evidence: access, admissibility and privacy.

### 5.2 Recommendations

(1) Definitions. Amend Motor Vehicles Act to define automated driving systems and their levels of automation and make the responsible entity liable for a given level, e.g., a licensed self-driving organization for Levels 4 and 5 and clear driver obligations for Levels 2 and 3. (2) Data loggers required. There needs to be a standardised, tamper-proof recording system for recording system engagement status, handover requests, alerts and pre-collision data, with specified retention periods and access for judicial bodies, investigators and insurers, in line with data protection regulations. (3) rebuttable presumptions which may be challenged. If the system was operational at the time of the incident and the manufacturer does not provide the necessary information, or if the incident would not typically happen if there was no defect, consider there to be a defect or causative factor in accordance with the EU directive. (4) Compensation without fault coupled with recovery. Keep mandatory insurance and no-fault indemnification to ensure timely payments to victims and give insurers a legal right of recourse against liable manufacturers and developers. (5) Product liability reform. Clarify that product liability covers embedded software, updates and AI components Ensure that bystanders have standing to sue (6) Safety standards. Set regulatory safety standards, perform pre-deployment assessments, carry out post-deployment surveillance, and encourage incident reporting, seeing compliance as a sign of due diligence, not an absolute safeguard. (7) Changed responsibility for crimes. It is essential to have clear statements of

the responsibilities of supervisors to the drivers. Corporate failings, including false claims of competence, should be met with violations of regulations, not with the expansion of reckless driving laws. (8) Organisation's capability. Provision of technical evaluators for tribunals and courts, training for judges and solicitors and allowing for limited pilot implementations only under a provisional liability regime.

## 6. CONCLUSION

AI driving does not eliminate negligence, but it does expose the assumptions upon which negligence rests. The duty of care can be extended to the designers and improvers of driving systems, violations can be recast as design and deployment decisions, and causation can be approached through apportionment and relaxed evidentiary standards. These changes, however, depend on proof of the current inability of the victims to obtain, and a legal terminology that Indian law has yet to create. If resolved by individual litigation, the result would likely be delay, uneven results, and a bias toward holding the individual closest to the vehicle responsible.

A hybrid approach is a viable solution. Laws assigning responsibility to a party in each step of automation. Rules for data documentation and transparency that allow for verification. Assumptions that correct information asymmetry. A no-fault insurance model that focuses on victim compensation and then spreads the costs. India is at a nascent stage and has the opportunity to learn these before major litigations erupt. Further research should monitor the emergence of Indian judgements and empirically test the proposals against accident and claims data.

## REFERENCES

1. SAE International, "Taxonomy and definitions for terms related to driving automation systems for on-road motor vehicles," SAE Int., Warrendale, PA, USA, Standard J3016_202104, Apr. 2021.
2. National Transportation Safety Board, "Collision between vehicle controlled by developmental automated driving system and pedestrian, Tempe, Arizona, March 18, 2018," NTSB, Washington, DC, USA, Rep. NTSB/HAR-19/03, Nov. 2019.
3. National Transportation Safety Board, "Collision between a sport utility vehicle operating with partial driving automation and a crash attenuator, Mountain View, California, March 23, 2018," NTSB, Washington, DC, USA, Rep. NTSB/HAR-20/01, Feb. 2020.
4. G. E. Marchant and R. A. Lindor, "The coming collision between autonomous vehicles and the liability system," Santa Clara Law Rev., vol. 52, no. 4, p. 1321, 2012.
5. B. W. Smith, "Automated driving and product liability," Mich. State Law Rev., vol. 2017, no. 1, p. 1, 2017.
6. R. Abbott, "The reasonable computer: Disrupting the paradigm of tort liability," George Washington Law Rev., vol. 86, no. 1, p. 1, 2018.
7. M. U. Scherer, "Regulating artificial intelligence systems: Risks, challenges, competencies, and strategies," Harvard J. Law Technol., vol. 29, no. 2, p. 353, 2016.
8. R. Calo, "Robotics and the lessons of cyberlaw," Calif. Law Rev., vol. 103, no. 3, pp. 513–563, 2015.
9. A. Matthias, "The responsibility gap: Ascribing responsibility for the actions of learning automata," Ethics Inf. Technol., vol. 6, no. 3, pp. 175–183, 2004.
10. A. Hevelke and J. Nida-Rümelin, "Responsibility for crashes of autonomous vehicles: An ethical analysis," Sci. Eng. Ethics, vol. 21, no. 3, pp. 619–630, 2015.

11. S. Gless, E. Silverman, and T. Weigend, "If robots cause harm, who is to blame? Self-driving cars and criminal liability," New Crim. Law Rev., vol. 19, no. 3, pp. 412–436, 2016.
12. M. C. Elish, "Moral crumple zones: Cautionary tales in human-robot interaction," Engaging Sci. Technol. Soc., vol. 5, pp. 40–60, 2019.
13. J. Burrell, "How the machine 'thinks': Understanding opacity in machine learning algorithms," Big Data Soc., vol. 3, no. 1, Art. no. 2053951715622512, 2016.
14. Y. Bathaee, "The artificial intelligence black box and the failure of intent and causation," Harvard J. Law Technol., vol. 31, no. 2, p. 889, 2018.
15. Law Commission and Scottish Law Commission, "Automated vehicles: Joint report," Law Com No. 404, Scot Law Com No. 258, HC 1068, Jan. 2022.
16. Automated Vehicles Act 2024 (UK).
17. Automated and Electric Vehicles Act 2018 (UK), c. 18.
18. Directive (EU) 2024/2853 of the European Parliament and of the Council of 23 October 2024 on liability for defective products, Off. J. Eur. Union, Nov. 18, 2024.
19. Motor Vehicles Act, 1988, Act No. 59 of 1988 (India).
20. Consumer Protection Act, 2019, Act No. 35 of 2019 (India).
21. Bharatiya Nyaya Sanhita, 2023, Act No. 45 of 2023 (India).
22. Bharatiya Sakshya Adhiniyam, 2023, Act No. 47 of 2023 (India).
23. Digital Personal Data Protection Act, 2023, Act No. 22 of 2023 (India).
24. Donoghue v. Stevenson, [1932] AC 562 (HL).
25. Caparo Industries plc v. Dickman, [1990] 2 AC 605 (HL).
26. Bolam v. Friern Hospital Management Committee, [1957] 1 WLR 582 (QBD).
27. Barnett v. Chelsea & Kensington Hospital Management Committee, [1969] 1 QB 428 (QBD).
28. Fairchild v. Glenhaven Funeral Services Ltd, [2002] UKHL 22, [2003] 1 AC 32.
29. Overseas Tankship (UK) Ltd v. Morts Dock & Engineering Co Ltd (The Wagon Mound (No. 1)), [1961] AC 388 (PC).
30. Shyam Sunder v. State of Rajasthan, (1974) 1 SCC 690 (India).
31. M. C. Mehta v. Union of India, (1987) 1 SCC 395 (India).
32. Jacob Mathew v. State of Punjab, (2005) 6 SCC 1 (India).
33. Anvar P. V. v. P. K. Basheer, (2014) 10 SCC 473 (India).
34. Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal, (2020) 7 SCC 1 (India).
35. Straßenverkehrsgesetz (Road Traffic Act), §§ 1a, 1b, 63a (Germany), as amended in 2017 and 2021.
36. Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence (Artificial Intelligence Act).
37. Benavides v. Tesla, Inc., jury verdict (S.D. Fla. Aug. 1, 2025).