CRIMINAL LIABILITY OF AUTONOMOUS VEHICLES

Snehpreet Kaur, LL.M. (Master of Laws), University Institute of Legal Studies, Chandigarh University, Mohali, Punjab, India.

Dr. Harshita Thalwal, Associate Professor, University Institute of Legal Studies, Chandigarh University, Mohali, Punjab, India

ABSTRACT

Automation in mobility disrupts long settled assumptions that anchor criminal fault to a human Automation in mobility destabilizes criminal law assumptions that locate fault solely in a human driver's choices and bodily acts. This paper studies Indian criminal law principles for the ascription of liability when an automated driving system (ADS) is performing the dynamic driving task, using doctrinal interpretation and comparative legislation as its sources of authority. It bases the core offences on the Bharatiya Nyaya Sanhita, 2023 (in particular, Sections 106 and 281), driver duties and recall powers in the Motor Vehicles Act, 1988 (Sections 134, 136, 110A and Rule 127C), evidentiary provisions in the Bharatiya Sakshya Adhiniyam, 2023 (Sections 61 63), search and seizure documentation under the Bharatiya Nagarik Suraksha Sanhita, 2023 (Section 105), privacy limitations in the Digital Personal Data Protection Act, 2023, and connectivity under the Telecommunications Act, 2023. The paper looks at the United Kingdom's Automated Vehicles Act 2024 (user in charge immunity and operator accountability) and the European Union's AI Act 2024 along with the new Product Liability Directive 2024 which extends no fault liability to software and tightens post market duties to compare the study. The results reveal that India has three gaps that continue to exist: (i) no AV specific offence which is allocation keyed to control states, (ii) ambiguity about a "user in charge" at conditional automation, and (iii) absence of an operator licensing layer. The paper suggests an India ready allocation based on SAE J3016 levels, a conditional safe harbor for a user in charge, statutory offences for the unsafe deployment of authorized entities/operators, and codified AV incident investigation protocols that align probative value with privacy protections. The proposal maintains the idea of fault-based culpability for any residual human roles at Levels 1 2, shifts 'manner of driving' exposure to authorized entities at Levels 3 4 within the ODD, and provides safety documented cases, timely recalls, and transparent data cooperation as incentives. These changes bring criminal attribution in line with real time control and governance while still keeping to India's high standard of criminal negligence.

Keywords - Autonomous vehicles, criminal liability, mens rea, negligence, Bharatiya Nyaya Sanhita, Motor Vehicles Act, user in charge, EU product liability, evidence, India

Introduction

The criminal law of roads has been built around human fallibility. Speed, intoxication, distraction, and risk-taking supply the characteristic facts of rashness or negligence. Autonomous vehicles unsettle that grammar by shifting the locus of control into software-defined systems that sense, decide, and act at machine timescales. Indian law presently treats vehicles as human-operated machines and deploys offences such as "Section 281 of the Bharatiya Nyaya Sanhita, 2023" for rash driving and "Section 106" for causing death by negligence, including an aggravated clause when a driver flees without reporting. These provisions remain vital where the human still performs supervision or intervenes late, yet they fit poorly when the control state renders human performance marginal or structurally eclipsed by the automated driving system. The "Motor Vehicles Act, 1988" sits in the foreground regulating licensing, construction and maintenance, driver duties after a crash under "Section 134", and, since 2019, a recall regime in "Section 110A" that can address systemic defects at scale. Still, the Act does not define or recognise autonomous driving as a distinct legal category, leaving criminal attribution to general offences conceived for a human driver, not a distributed cyber-physical agent.[1]

The information substrate of AV operation also forces a rethinking of evidence and privacy. Event data recorders, driver monitoring feeds, planning traces, and connectivity logs are personal data and digital records. Processing such data for crash investigation must align with the "Digital Personal Data Protection Act, 2023", while admissibility and proof must traverse "Sections 61 to 63" of the "Bharatiya Sakshya Adhiniyam, 2023", which confirm that electronic or digital records carry equal legal effect subject to statutory conditions. The "Bharatiya Nagarik Suraksha Sanhita, 2023" reinforces reliability through mandated audio-video recording of search and seizure under "Section 105". This converges with the "Telecommunications Act, 2023", which consolidates the legal basis for telecommunication services and networks that underpin V2X connectivity, spectrum assignment, and lawful interception safeguards. A criminal-law response to AVs in India must therefore braid together

[1] Jacob Turner, *Robot Rules: Regulating Artificial Intelligence* 198 (Palgrave Macmillan, London, 1st edn., 2019).

offences, sectoral regulation, data protection, telecommunications, and evidence rules into a coherent framework that tracks control allocations across SAE levels and deployment contexts.[2]

Research Questions

The research questions for the study are as follows –[3]

1. How should negligence, knowledge, and recklessness under the "Bharatiya Nyaya Sanhita, 2023" apply when an automated driving system performs the dynamic driving task and the human supervisor's role is residual or intermittent?[4]

2. To what extent should corporate and vicarious liability principles attach to manufacturers, software suppliers, and operator entities when accidents result from foreseeable system failure modes, unsafe deployment, or disregard of known defects?

3. How should the calibration of fault correspond to SAE levels, the legal status of a user in charge, and the need for operator licensing?

4. How can evidentiary and privacy constraints be integrated in digital investigations under the BSA, BNSS, and the DPDP Act?

Problem Statement

India lacks an AV-specific criminal liability regime. The present practice applies general offences for rash driving and causing death by negligence to events where automation performs core driving functions. This misalignment creates uncertainty over attribution among a human supervisor who may not be continuously engaged, a fleet operator or authorised entity that configures and monitors software behaviours, and a manufacturer that controls updates and safety cases. Absent definitions for self-driving and a user in charge within the Motor Vehicles framework, and without operator licensing, enforcement risks both over-penalising residual humans and under-deterring unsafe system deployment across public roads.[5]

[2] The Digital Personal Data Protection Act, 2023, available at: https://www.meity.gov.in/static/uploads/2024/06/2bf1f0e9f04e6fb4f8fef35e82c42aa5.pdf (last visited on October 28, 2025).
[3] Andrew Ashworth, *Principles of Criminal Law* 162 (Oxford University Press, Oxford, 1st edn., 2013).
[4] *Supra* note 3.
[5] Dorothy J. Glancy, "Privacy in Autonomous Vehicles", 52 *Santa Clara Law Review* 1171 (2012).

Objectives of the Study

The objectives of the study are as follows –[6]

1. To clarify doctrinal standards for negligence, knowledge, and recklessness in AV contexts under the "Bharatiya Nyaya Sanhita, 2023" and to evaluate foreign approaches, including the United Kingdom's "Automated Vehicles Act 2024" and the European Union's AI and product liability reforms, for their transposability to Indian conditions.[7]

2. To propose an India-ready allocation of criminal fault across actors and automation levels, including an explicit user-in-charge concept, an operator licensing layer, and specific manufacturer and operator-facing offences for unsafe deployment, while harmonising evidentiary and privacy demands under the BSA, BNSS, DPDP Act, and the Telecommunications framework.

Research Methodology

This is a doctrinal and comparative study that interrogates statutes, official policy papers, and scholarly commentary without empirical fieldwork. Primary sources include India Code texts of the "Bharatiya Nyaya Sanhita, 2023", the "Motor Vehicles Act, 1988", the "Bharatiya Sakshya Adhiniyam, 2023", the "Bharatiya Nagarik Suraksha Sanhita, 2023", the "Digital Personal Data Protection Act, 2023", and the "Telecommunications Act, 2023". Comparative sources include the "Automated Vehicles Act 2024" of the United Kingdom, the "EU Artificial Intelligence Act 2024", and the "EU Product Liability Directive 2024". Policy synthesis draws on the PRS Science and Technology brief on autonomous vehicles and technical references to the SAE J3016 taxonomy for control states.[8]

Technology and Control States

Automation exists along a continuum. The SAE J3016 taxonomy distinguishes driver support at Levels 1 and 2 from automated driving at Levels 3 to 5. The legal salience of this taxonomy

[6] SAE Levels of Driving Automation, available at: https://www.sae.org/news/blog/sae-levels-driving-automation-clarity-refinements (last visited on October 27, 2025).
[7] *Supra* note 6.
[8] Ugo Pagallo, *The Laws of Robots: Crimes, Contracts, and Torts* 173 (Springer, Dordrecht, 1st edn., 2013).

lies in control allocation. At driver support, the human must continuously supervise and perform fallback. At conditional automation, the system performs the dynamic driving task but expects a user in charge to respond to take-over requests within specified limits. At high automation, the system can operate without human fallback within the operational design domain. The criminal law must track these differences because fault presupposes agency over risk-creating decisions. Where agency lies chiefly in software, the inquiry must move from traditional rashness to foreseeability of system failure and governance of updates.

Sae Levels and Human Role

Driver assistance and self-driving are not synonyms. In driver assistance, lane keeping or adaptive cruise control acts as servo support, with the human continuously responsible for observation, prediction, and planning. In self-driving, the automated driving system performs these functions, drawing on fused sensor perception and high-definition maps to localise, predict agents, and plan trajectories. The law must therefore differentiate a driver who ignores salient hazards from a user in charge who faces automation surprise or a stale map defect outside human foresight. The conceptual user in charge appears explicitly in the United Kingdom's "Automated Vehicles Act 2024", which grants immunity for the manner of driving when the self-driving feature is engaged, shifting exposure to authorised self-driving entities except in defined exception conditions. That legislative choice recognises that control sits with the system, not the human, during engagement, and it offers a template for calibrated Indian reform.[9]

Av Stack and Failure Modes

The AV stack comprises perception, prediction, planning, and actuation, supported by high-definition maps and, in connected modes, V2X messages. Perception fuses LiDAR, radar, and camera signals to produce an object list and state estimates. Prediction generates hypotheses on trajectories of vehicles, cyclists, and pedestrians under uncertainty. Planning selects trajectories that satisfy safety envelopes and traffic rules before issuing control outputs to actuators. High-definition maps deliver prior knowledge of lane geometry, traffic control devices, and drivable space; they act as a long-range sensor and strongly influence behaviour in occluded or complex scenes. Typical failure scenarios include sensor occlusion or glare, map

[9] Automated Vehicles Act 2024, available at: https://www.legislation.gov.uk/ukpga/2024/10/contents (last visited on October 27, 2025).

staleness, misclassification of vulnerable road users, or adversarial edge cases at unprotected turns. Foreseeability turns on whether these modes were known, mitigated by design or updates, and properly guarded by driver monitoring where supervision remains expected.[10]

System Error vs Human Error

Traditional rashness and negligence standards focus on human choices like speed, intoxication, and inattention. In an automated system, decisions are algorithmic, distributed, and sometimes opaque by design. That complicates mens rea because the immediate agent is software executing a policy optimised over training data and safety constraints. Human supervisors may face low-arousal vigilance tasks that degrade situational awareness, while system safeguards like driver monitoring attempt to keep the human engaged. Criminal law must avoid treating structural automation limits as if they were individual moral failings while still preserving accountability. The analysis must examine whether the system's foreseeable failure modes were addressed, whether safety cases documented risk trade-offs, and whether residual human roles were realistically supported by interface design. The fault line therefore runs through governance choices by operator entities and manufacturers as much as through any momentary lapse by a user in charge in conditional automation.[11]

Indian Legal Framework

The Indian legal landscape already contains many of the building blocks needed to address criminal liability around AVs, yet it lacks a targeted allocation scheme that reflects control states. The "Bharatiya Nyaya Sanhita, 2023" offers substantive offences like "Section 106" for causing death by negligence, including an aggravated clause for rash and negligent driving coupled with escape without reporting, and "Section 281" for rash driving on a public way.[12] The "Motor Vehicles Act, 1988" regulates drivers, construction and maintenance of vehicles, duties after accidents, and, after the 2019 amendment, recall and type-approval oversight that can address systemic defects. The "Bharatiya Sakshya Adhiniyam, 2023" sets the evidentiary baseline for admitting digital records, while the "Bharatiya Nagarik Suraksha Sanhita, 2023" modernises search and seizure with audio-video capture. The "Digital Personal Data Protection

[10] Online High-Definition Map Construction for Autonomous Vehicles: A Comprehensive Survey, available at: https://www.mdpi.com/2224-2708/14/1/15 (last visited on October 25, 2025).
[11] Matthew U. Scherer, "Regulating Artificial Intelligence Systems: Risks, Challenges, Competencies, and Strategies", 29 *Harvard Journal of Law and Technology* 353 (2016).
[12] Sven A. Beiker, "Legal Aspects of Autonomous Driving", 52 *Santa Clara Law Review* 1145 (2012).

Act, 2023" frames lawful grounds and safeguards for processing personal data present in AV logs, and the "Telecommunications Act, 2023" enables connectivity and spectrum governance foundational to V2X safety.

Substantive Offences under BNS 2023

"Section 106 of the Bharatiya Nyaya Sanhita, 2023" criminalises causing death by a rash or negligent act not amounting to culpable homicide and adds an aggravated clause for "rash and negligent driving of vehicle" where the person escapes without reporting to police or a Magistrate, with punishment that may extend to ten years and fine. "Section 281" punishes rash or negligent driving or riding on a public way where human life is endangered or injury is likely, with imprisonment up to six months or fine or both. These offences can already anchor prosecutions arising from AV incidents where a human remains the legal driver or where a user in charge fails to meet residual duties such as take-over or post-crash reporting. Calibration becomes complex when control is allocated to the system and the human's realistic capacity to avoid harm is low, raising the case for corporate attribution where foreseeability and governance are shown.[13]

Motor Vehicles Act and Rules

The "Motor Vehicles Act, 1988" regulates licensing, construction and maintenance, traffic control, accident duties, insurance, and recall. "Section 134" continues to impose a duty on the driver to stop and render assistance in case of an accident. Post-2019, "Section 110A" empowers the Central Government to direct recall of motor vehicles of a particular type or variant where a defect may cause harm to road users, the environment, or the driver or occupants, and the Central Motor Vehicles Rules include "Rule 127C" prescribing the recall procedure. Type-approval and testing duties interact with recall through related provisions to ensure conformity and remediation. The Act has not yet defined autonomous driving or created an operator licensing layer, so AV deployments must be fitted into the existing categories for drivers and vehicles, with criminal liability flowing through general offences and driver duties not specifically tuned to automated control states.

[13] Peter Cane, Atiyah's Accidents, *Compensation and the Law* 190 (Cambridge University Press, Cambridge, 1st edn., 2013).

Data and Networks Touchpoints

The "Digital Personal Data Protection Act, 2023" governs the processing of digital personal data present in event data recorders, driver monitoring systems, and software logs used in AV investigations. Lawful processing grounds and duties of data fiduciaries constrain access and disclosure of identifiable data, while exemptions and legitimate uses must be interpreted tightly in the criminal justice setting. The admissibility and proof of these digital records sit within "Sections 61 to 63" of the "Bharatiya Sakshya Adhiniyam, 2023", which recognise electronic or digital records and set out conditions for computer outputs. The "Telecommunications Act, 2023" consolidates the legal basis for telecommunication services and networks, assignment of spectrum, and related matters incidental to V2X connectivity, whose reliability and lawfulness affect safety and liability. Together, these statutes form the backbone for privacy-preserving yet probative use of AV data in criminal proceedings.[14]

Policy Posture

India's policy discussion reflects the complex integration of AVC regulations across different domains but at the same time it points out that there is no specific regime for criminal liabilities specially designed for automated driving. The PRS Science and Technology brief on autonomous vehicles mentions that currently, criminal provisions cover cases of negligent or rash driving, and mandatory insurance provides civil compensation. However, there is still the question of determining liability if the harm is due to automation rather than a direct human fault. Such a finding paves the way for a legislative journey that describes operation of a self-driving vehicle, introduces a user in control if local conditions allow, and transfers at least some offences and compliance obligations to operator entities and manufacturers who authorize and supervise deployment.[15]

Mens Rea and Attribution

Mens rea categories in the "Bharatiya Nyaya Sanhita, 2023" must be translated to the socio-technical context of AVs. Negligence revolves around failure to exercise reasonable care in circumstances where a duty exists and harm is foreseeable. Knowledge and recklessness imply

[14] Motor Vehicles Act Resources, available at: https://lawmin.gov.in/ (last visited on October 24, 2025).
[15] Science and Technology Policy Brief: Autonomous Vehicles, available at: https://prsindia.org/policy/science-technology-brief/science-technology-policy-brief-autonomous-vehicles (last visited on October 23, 2025).

awareness of risks and conscious disregard. The critical doctrinal move is to locate the actor who controls the risk at the time of decision. When the automated driving system executes the driving task, the focus should widen beyond a human's momentary lapse to include operator entities and manufacturers whose choices about deployment, updates, and monitoring materially shape risk. Indian law has the conceptual tools to attribute liability to corporations through vicarious and direct responsibility doctrines in appropriate cases; the challenge is to specify triggers in AV contexts tied to control states and safety cases, while maintaining fair treatment for residual human roles in conditional automation.[16]

Negligence, Knowledge, and Recklessness

Negligence under "Section 106" in a driving context has long assessed whether the accused failed to conform to a standard of reasonable care given the circumstances. In automated operation, that standard must be applied to the human supervisor only to the extent the design affords meaningful control. Where a safety driver is tasked with continuous vigilance at Level 2, or with timely take-over at Level 3, failure to attend, respond to alerts, or comply with post-accident reporting may evidence negligence or knowledge of risk where distraction or intoxication is proven. For remote operators and fleet managers, mens rea turns on documented knowledge of known defects, ignored safety advisories, or decisions to continue operation after critical fault codes. For automated mode mishaps, the inquiry should examine whether the system's failure modes were foreseeable and mitigated through updates and driver monitoring; where deployment proceeded despite known safety gaps, recklessness may be argued against the operator entity or responsible officers.[17]

Corporate and Vicarious Liability

Corporate criminal liability in India recognises that companies act through individuals while maintaining separate personality. In AV contexts, attribution should track organisational decisions that authorise deployment, define operational design domains, schedule updates, and set driver monitoring thresholds. If a manufacturer or software supplier disseminates an update that disables or weakens safety constraints, or fails to address a known defect identified through field incidents or recall investigations under "Section 110A of the Motor Vehicles Act, 1988",

[16] Bryant Walker Smith, "Automated Vehicles Are Probably Legal in the United States", 1 *Texas A&M Law Review* 411 (2014).
[17] AI Liability Directive Proposal, available at: https://digital-strategy.ec.europa.eu/en/policies/ai-liability-directive (last visited on October 23, 2025).

direct liability may follow where statutory duties or general offences are engaged. Operator entities that dispatch vehicles beyond certified operational envelopes or ignore driver monitoring alerts that evidence chronic non-compliance may face liability where negligence or knowledge can be proved through logs and safety case documentation. Individual officers may be liable in defined cases that meet statutory criteria and proof thresholds, but doctrine should avoid strict transposition of vicarious liability in the absence of clear statutory direction calibrated to AV operations.[18]

Strict vs Fault Based Models

When discussing strict versus fault based criminal liability, one should take into account the control and information asymmetries. A fault-based system would continue to apply to human supervisors at Levels 2 and 3, as it acknowledges their ability and responsibility to oversee and react. In the case of Levels 3 to 4, where the system is performing the dynamic driving task, the offences in the case of the driving should be those of the operator entity or the authorized self-driving entity with the human liability being only for supervisory neglect or interference. It may be the case that corporate actors are held strictly liable for their breaches of core safety provisions where such public welfare considerations and recall regimes intersect, but it should be accompanied by defenses based on due diligence and compliance with approved safety cases. This tiering reflects the United Kingdom's model where a person in control is not responsible for the way the vehicle is driven when the feature is on, except for certain cases, and the responsibility changes to the authorized entities.

Compliance and Safety Case Defences

Safety cases detailing hazards, mitigations, verification evidence, and in service monitoring can thus be termed as 'evidentiary shields' for operator entities and manufacturers in the case of incidents which are a result of diligent governance, but still arise. As per the "Bharatiya Sakshya Adhiniyam, 2023", digital records of tests, simulations, incident triage, and corrective updates are considered as evidence subject to "Sections 61 to 63". In cases where organizations are able to demonstrate the implementation of fixes in a timely manner, cooperation in recall under "Section 110A of the Motor Vehicles Act, 1988" and driver monitoring activities being

[18] Section 110A Recall of Motor Vehicles, available at: https://www.indiacode.nic.in/show-data?actid= AC_CEN_30_42_00009_198859_1517807326286&orderno=119&sectionId=50174&sectionno=110A (last visited on October 22, 2025).

carried out in an effective manner, then culpability can be lessened. On the other hand, inadequate documentation, delayed updates, concealment of crash data, and avoidance of recall obligations contribute to the aggravation of fault. Indian legal principles should enact a compliance defense for AVs which is in line with the management of safety cases and continuous improvement while at the same time allowing for prosecution if governance falls below reasonable standards or shows a conscious disregard of risk.[19]

Comparative Perspectives

Comparative regimes reveal two broad moves. First, where a vehicle is self-driving as defined by public authorisation, many jurisdictions shift liability from a human occupant to an entity responsible for the automated feature. Second, product and AI regulation build compliance scaffolding that indirectly shapes criminal risk by clarifying duties, documentation, and post-market monitoring. The United Kingdom makes the clearest statutory allocation via the "Automated Vehicles Act 2024". The European Union's "AI Act 2024" and the new "Product Liability Directive 2024" modernise baseline expectations and expand no-fault product liability to software and AI, adding discovery, presumptions, and post-sale update duties that will condition corporate behaviour and, by extension, prosecutorial narratives around knowledge and recklessness. United States practice shows case-by-case prosecutions of human drivers or supervisors in automated mode, with civil verdicts influencing corporate responses and safety messaging.[20]

United Kingdom

The "Automated Vehicles Act 2024" establishes an authorisation regime for self-driving features, defines a "user-in-charge", and then provides that a user in charge is not liable for the manner of driving while the self-driving feature is engaged. The Act carves exceptions for duties that remain with the user in charge, such as insuring the vehicle and responding to police directions, and it retains liability where the feature is misused or where the user ignores a lawful instruction to retake control. Responsibility for driving offences and safety failures during engagement pivots to authorised self-driving entities and licensed operators, backed by enforcement and sanctions calibrated to compliance failures. This statutory design directly

[19] The Bharatiya Sakshya Adhiniyam, 2023, available at: https://www.indiacode.nic.in/bitstream/123456789/20063/1/a2023-47.pdf (last visited on October 21, 2025).
[20] Roger Brownsword, Eloise Scotford, et.al., *The Oxford Handbook of Law, Regulation and Technology* 211 (Oxford University Press, Oxford, 1st edn., 2017).

addresses the control problem by aligning criminal exposure with the entity that actually decides how the vehicle behaves while self-driving.[21]

European Union

The "EU Artificial Intelligence Act 2024" is a legislative regulation that identifies and sets different risk-based rules for AI systems, including those in vehicles, in areas such as data management, transparency, and after market surveillance. Moreover, the "Product Liability Directive 2024" goes back to the 1985 directive and introduces non fault liability for software and AI, thus broadening the definition of the product, introducing production and discovery obligations, and creating presumptions of defect and causation in the case of technical issues. Although these are civil law instruments, they change the AVs' corporate governance environment, thus determining which practices are considered reasonable and by criminal inquiries, narrowing the inferences of knowledge or disregard. For Indian policymakers, these laws serve as examples of how a compliance framework can facilitate proper criminal attribution without requiring an extension of traditional mens rea categories.[22]

United States

Criminal charges against the human operator or a supervisor in an automated or driver assistance mode where the driver was distracted, intoxicated, or failed to supervise have been the main focus of American prosecutors. After the fatal test vehicle crash sentencing of the Uber safety driver in Arizona for endangerment, the plea and sentencing of the safety driver in Arizona for endangerment after the fatal test vehicle crash and the Los Angeles County case where a Tesla driver pleaded no contest to vehicular manslaughter are examples of this line. Among other things, large civil verdicts, such as the one awarded by a Florida jury in 2025, which exceeded 240 million dollars and was directed against Tesla with corporate fault to some extent, add the background incentives that influence the corporate safety choices and disclosures. This pattern shows that criminal exposure in partial automation is still human centered, while civil litigation is a pressure on manufacturers to make representations, updates,

[21] Kyle Graham, "Of Frightened Horses and Autonomous Vehicles: Tort Law and its Assimilation of Innovations", 52 *Santa Clara Law Review* 1241 (2012).
[22] Regulation (EU) 2024/1689 Artificial Intelligence Act, available at: https://eur-lex.europa.eu/eli/reg/2024/1689/oj/eng (last visited on October 20, 2025).

and safety governances.[23]

Lessons for India

The comparative record supports a layered approach. An explicit user-in-charge concept should sit alongside a licensing layer for operator entities that authorise self-driving deployment. Where a self-driving feature is engaged, offences tied to the manner of driving should generally attach to the authorised entity or licensed operator, not the user in charge, save for clearly defined exception duties. Corporate offences should address unsafe deployment, failure to update known defects, breach of safety cases, and concealment of crash data. The Motor Vehicles framework should be amended to define self-driving, to recognise authorised entities, and to mesh recall and type-approval with operator obligations. Insert Comparison Table 4 here: "Criminal liability allocation in UK, EU, US, India."[24]

Case Law Analysis

Indian and foreign decisions on negligent killing and hazardous driving provide the doctrinal scaffolding for calibrating criminal liability around autonomous vehicles. The thread that runs through leading Indian authorities is the insistence on a demanding threshold for criminal negligence, reserving penal censure for conduct that departs grossly from reasonable care. That threshold matters when supervision is technologically attenuated or when risk control sits with an automated driving system and its corporate sponsors. Foreign criminal proceedings involving automated and semi-automated operation show prosecutors focusing on human monitors in partial automation and reserving corporate exposure to civil fora or regulatory action. Read against "Section 106 of the Bharatiya Nyaya Sanhita, 2023" and "Section 281 of the Bharatiya Nyaya Sanhita, 2023", these cases illuminate how knowledge, recklessness, and negligence travel when the dynamic driving task is no longer purely human.[25]

Alister Anthony Pareira v. State of Maharashtra,

In the case of "*Alister Anthony Pareira v. State of Maharashtra*[26], the Supreme Court had before

[23] Driver of Uber Vehicle Involved in Death of Woman in Tempe Pleads Guilty, available at: https://maricopacountyattorney.org/CivicAlerts.aspx?AID=1012 (last visited on October 19, 2025).
[24] Kevin Funkhouser, "Paving the Road Ahead: Autonomous Vehicles, Products Liability, and the Need for a New Approach", 2013 *Utah Law Review* 437 (2013).
[25] Jacob Mathew vs State of Punjab & Anr on 5 August, 2005, available at: https://indiankanoon.org/doc/871062/ (last visited on October 28, 2025).
[26] (2012) 2 SCC 648.

it a tragic case of a late-night car crash in Mumbai. Several people sleeping on a pavement were killed as the vehicle went out of control and mounted the curb. According to the prosecution story, the factors leading to the accident were alcohol consumption, speed, and the indifference of the driver. The trial court hearing and the appeals also looked into whether the incident was only a case of negligence causing death or if there was knowledge of the likelihood of death due to the combination of intoxication, loss of control, and a serious result. The different levels of factual reconstruction dealt with the collision and control opportunities and the driver's condition. They also referred to the aggravating features being given more importance than the ordinary kind of rashness. The procedural journey of the case indicated a change in the degrees of culpability as the courts considered whether the mental element was above simple negligence.[27]

State of Arizona v. Rafaela Vasquez (Uber Safety Driver), 2023 Plea and 2024 Sentence

In the case of "State of Arizona v. Rafaela Vasquez", the fatal 2018 Tempe crash involving an Uber self-driving test vehicle formed the backdrop for a prosecution focused on the human safety driver's supervision. The vehicle, operating in an automated test mode on a public road, struck a pedestrian crossing a multi-lane arterial at night. Investigators examined in-cabin monitoring, roadway lighting, pedestrian behavior, and system logs, but the criminal information targeted the safety driver's conduct during automated operation. The defendant pleaded guilty in July 2023 to a single count of endangerment under Arizona law, acknowledging exposure created by a failure to maintain the vigilance expected during testing. The case condensed a complex automated stack into a human-centered charge that prosecutors could advance within familiar doctrines and proof structures rather than attempting an untested corporate homicide theory for experimental software behavior.[28]

People v. Kevin George Aziz Riad, Los Angeles County, 2019 Crash

In the case of "People v. Kevin George Aziz Riad", prosecutors charged the driver of a Tesla Model S involved in a December 2019 Gardena crash that killed two occupants of a Honda Civic after the Tesla ran a red light at high speed while Autopilot was reportedly engaged. The

[27] Alister Anthony Pareira vs State of Maharashtra on 12 January, 2012, available at: https://indiankanoon.org/doc/79026890/ (last visited on October 27, 2025).
[28] Rafaela Vasquez Pleads Guilty in Fatal Uber Self-Driving Crash That Killed Pedestrian Elaine Herzberg, available at: https://www.azcentral.com/story/news/local/tempe/2023/07/28/rafaela-vasquez-pleads-guilty-in-in-fatal-uber-self-driving-crash-killed-pedestrian-elaine-herzberg/70488361007/ (last visited on October 26, 2025).

proceeding gained attention as an early felony prosecution of a driver using a partially automated driver-assistance feature. Pretrial rulings confirmed sufficient cause to proceed to trial on two counts of vehicular manslaughter, with evidence concerning speed, signal violation, and system engagement forming a contested matrix around human responsibility in a driver-assistance context. The case signposted that partial automation would not shield a human driver from traditional driving offences where the human remained expected to monitor and obey traffic controls.[29]

Recent Civil Verdicts Against OEMs

In the case of "Benavides Leon v. Tesla, Inc. (jury verdict, S.D. Fla.)", a Florida federal jury in August 2025 awarded a total exceeding two hundred forty million dollars after finding Tesla partially responsible for a 2019 fatal crash involving a Model S operating with Autopilot. Public reports indicate the jury allocated roughly one third of compensatory fault to Tesla and assessed punitive damages of two hundred million dollars, while attributing remaining responsibility to the human driver who was distracted by a cell phone. The verdict arrived after plaintiffs alleged overstatement of Autopilot capabilities and concealment of critical crash data. Tesla denied wrongdoing and announced an appeal, contending that driver misconduct and unavoidable dynamics caused the harm. Although civil rather than criminal, the verdict reframes corporate knowledge and safety messaging in a way that could influence criminal narratives about recklessness or knowledge if analogous facts were proved in a penal forum, especially where updates, warnings, and post-crash disclosures are shown to be deficient.[30]

Allocation Framework for India

An allocation framework for India should align criminal exposure with real-time control and governance responsibility while maintaining a principled threshold for criminal negligence. The "Bharatiya Nyaya Sanhita, 2023" already contains offences capable of addressing negligent killing and rash driving, but fairness and deterrence require mapping those offences to control states so that a user in charge is not unfairly burdened when system agency predominates. The "Motor Vehicles Act, 1988" should supply definitions and licensing for

[29] Driver of Tesla on Autopilot Must Stand Trial for Crash that Killed 2 in Gardena, Judge Rules, available at: https://abc7.com/post/tesla-gardena-crash-driver/11873142/ (last visited on October 25, 2025).
[30] Tesla Rejected 60 Million Settlement Before Losing 243 Million Autopilot Verdict, available at: https://www.reuters.com/legal/litigation/tesla-rejected-60-million-settlement-before-losing-243-million-autopilot-verdict-2025-08-25/ (last visited on October 23, 2025).

authorized entities operating self-driving features and connect recall and type-approval with criminally relevant duties to update, monitor, and disclose. The "Bharatiya Sakshya Adhiniyam, 2023", the "Bharatiya Nagarik Suraksha Sanhita, 2023", the "Digital Personal Data Protection Act, 2023", and the "Telecommunications Act, 2023" should frame a disciplined approach to digital evidence, lawful processing, and V2X dependencies so that proof and privacy move in tandem with safety. The framework that follows is designed to be modular, level-contingent, and compatible with established Indian doctrines on mens rea and corporate attribution.[31]

Level Contingent Liability

Tiering liability by SAE level connects culpability to feasible human agency and to corporate control of software behavior. For Levels 1 and 2, where the human remains the continuous driver, traditional offences under "Section 281 of the Bharatiya Nyaya Sanhita, 2023" and "Section 106 of the Bharatiya Nyaya Sanhita, 2023" should apply to red light violations, speeding, intoxication, and post-crash derelictions, supported by driver-monitoring and signal-compliance records. For Level 3 with a user in charge, liability should narrow to supervisory neglect proven through alerts ignored, intoxication, or knowing misuse, while the manner of driving during engagement should pivot to the operator entity's risk governance when failure modes were foreseeable and uncorrected. For Levels 4 and 5 within an authorized operational design domain, criminal exposure for the manner of driving should reside primarily in the authorized entity and licensed operator, with corporate officers answerable where statutes so provide and were proof shows participation or knowledge of unsafe deployment. This allocation respects Indian culpability structures while recognizing software agency.[32]

User in Charge Safe Harbour

A conditional safe harbor for a user in charge should be codified so that, when a certified self-driving feature is engaged as designed, the user in charge is not liable for the manner of driving, save for defined residual duties such as sobriety, insurance, compliance with police directions, and responsive take-over when lawfully demanded. This approach mirrors the logic of the United Kingdom's regime while adapting it to Indian offences and enforcement practice under

[31] Mark A. Geistfeld, "A Roadmap for Autonomous Vehicles: State Tort Law Should Align With Federal Safety Regulations", 105 *California Law Review* 1611 (2017).
[32] SAE J3016 Taxonomy and Definitions, available at: https://www.sae.org/standards/j3016_202104-taxonomy-definitions-terms-related-driving-automation-systems-road-motor-vehicles (last visited on October 28, 2025).

"Section 281 of the Bharatiya Nyaya Sanhita, 2023" and "Section 106 of the Bharatiya Nyaya Sanhita, 2023". The safe harbor should be linked to an operator licensing layer within the "Motor Vehicles Act, 1988", with authorized entities bearing duties to maintain safety cases, deploy updates addressing known hazards, and disclose incident data lawfully for criminal investigations under the "Bharatiya Sakshya Adhiniyam, 2023" and the "Digital Personal Data Protection Act, 2023". Calibrated exceptions should capture misuse, tampering, and refusal to retake control when properly instructed.[33]

Corporate and Operator Culpability

Corporate and operator culpability should turn on governance choices that shape real-time risk, not on metaphors that personify machines. The "Motor Vehicles Act, 1988" already supplies levers that speak to systemic defects and post-market vigilance, including "Section 110A" on recall and "Rule 127C" of the Central Motor Vehicles Rules prescribing recall procedure. When an authorized entity deploys software that it knows, or ought to know, will encounter a foreseeable failure mode within its declared operational design domain, criminal attribution should consider whether the entity maintained a living safety case, triaged incidents, and acted on recall triggers in good time. Where an operator persists in public-road operation after field signals of critical hazard, direct fault can be articulated without straining doctrine. Complementary duties should flow from accident-handling provisions like "Section 134" and inspection powers under "Section 136", which shape expectations about post-crash conduct and cooperation. These statutory touchpoints support calibrated corporate exposure when unsafe deployment or concealment materially aggravate risk.[34]

Draft Offence Map and Penalties

An offence map for India should mirror BNS gradations while shifting locus where the automated feature governs behavior. For Levels 1 and 2, traditional driving offences under "Section 281 of the Bharatiya Nyaya Sanhita, 2023" and negligent killing under "Section 106" remain primary anchors, with corporate exposure limited to exceptional scenarios like knowingly defective components tied to crash causation. For Level 3 within a certified domain, the manner of driving during engagement should pivot to the authorized entity or licensed

[33] Matthew Channon, Lucy McCormick, et.al., *The Law and Autonomous Vehicles* 182 (Routledge, London, 1st edn., 2019).
[34] Eugene Volokh, "Tort Law vs. Privacy", 114 *Columbia Law Review* 879 (2014).

operator where failure modes were foreseeable, while the user in charge answers only for supervisory dereliction or intoxication. For Levels 4 and 5, offences concerning the manner of driving should attach to the authorized entity and its responsible officers where statutes so specify, with due-diligence defenses keyed to documented safety cases and recall compliance.

Enforcement and Evidence

Enforcement quality will decide whether criminal attribution around automated driving is fair and credible. Digital traces from event data recorders, driver monitoring systems, planning logs, and connectivity will anchor both charging decisions and trials. The "Bharatiya Sakshya Adhiniyam, 2023" places electronic and digital records on a statutory footing through "Sections 61 to 63", while the "Bharatiya Nagarik Suraksha Sanhita, 2023" mandates audio-video recording of search and seizure under "Section 105". These instruments, read with accident-duties and inspection powers in the "Motor Vehicles Act, 1988", build a lawful path to acquiring, preserving, and presenting subsystem evidence without eroding privacy guarantees. The "Digital Personal Data Protection Act, 2023" and the "Telecommunications Act, 2023" supply the parallel data and network law scaffolding required for V2X-dependent investigations. Together, they define a chain from on-road incident to courtroom proof that respects both integrity and rights.[35]

Digital Evidence and Privacy

Digital traces in accidents involving AV combine different kinds of data that include personal data and very detailed technical logs. Lawful processing of this data demands that there is a definite basis under the "Digital Personal Data Protection Act, 2023", that there is a careful minimization of the data, and that there is purpose limitation during each stage, i.e., extraction, analysis, and disclosure. Investigators should use "Section 105 of the Bharatiya Nagarik Suraksha Sanhita, 2023" for audio and video recording of the seizure of EDUs, storage media, and connectivity modules that in turn help to create the custody which can be traced and verified. Admissibility and weight thus move from the "Sections 61 to 63" of the "Bharatiya Sakshya Adhiniyam, 2023" that deal with the recognition of electronic and digital records and the setting of conditions for computer outputs. In the case of V2X messages that are used for giving situational awareness, the "Telecommunications Act, 2023" is the one that defines

[35] Ian Walden, *Computer Crimes and Digital Investigations* 168 (Oxford University Press, Oxford, 1st edn., 2007).

network legality and interception safeguards. All these statutory provisions interlinked together facilitate the use of EDR snapshots, driver monitoring clips, and planning traces as evidence while keeping in check over collection and also strengthening the trust in the recorded seizure through the structured certification.[36]

Investigative Protocols

Errors in Specialized AV crash protocols should be minimized by codifying such protocols and the evidence should be strengthened. Inspection of vehicles involved in accidents through "Section 136" is already provided for in the "Motor Vehicles Act, 1988" and can be broadened by the rules to incorporate capture of software state, firmware baselining, and secure storage imaging. If there is a need to extract the data, the investigators should do it under "Section 105" of the BNSS with their work being recorded through the audio video capture continuously. They should then seal and hash datasets in order to keep the chain of custody that can be verified. A nationwide template should indicate the procedure of obtaining time synchronized logs from perception, prediction, planning, and actuation modules as well as the way to keep configuration and calibration files and to link with roadside CCTVs and V2X records in accordance with the "Telecommunications Act, 2023". Inconsistencies resolved through recall and defect management under "Section 110A" will be a source of systemic solutions where patterns become evident. The methodology enhances the trustworthiness of the steps taken from the roadside recovery to the courtroom reconstruction.[37]

Expert Testimony and Standards

Expert testimony should help the court to understand the complicated evidence by providing risk narratives that are clear and that do not give an impression of too much certainty. The baseline of evidence in the "Bharatiya Sakshya Adhiniyam, 2023" recognizes digital records as legally significant, but the core of the persuasion will be experts who can identify the connection of failure modes to safety case assumptions and control allocation at the moment of the incident. Reference taxonomies such as SAE J3016 can help the tribunal understand the expected human role at each level of automation. National guidance can use type approval and recall literature under the "Motor Vehicles Act, 1988", as well as operator safety case

[36] Orin S. Kerr, "A User's Guide to the Stored Communications Act, and a Legislator's Guide to Amending It", 72 *George Washington Law Review* 1208 (2004).
[37] Section 136 Inspection of Vehicle Involved in Accident, available at: https://indiacode.nic.in/show-data?actid=AC_CEN_30_42_00009_198859_1517807326286&orderno=147 (last visited on October 21, 2025).

documentation, to derive safety expectations about verification, validation, and in service monitoring. Court will expect the presence of well-organized explanations of perception blind spots, stale map impacts, and take over dynamics, which should be grounded in logs rather than being the court's speculation. This disciplined interface between engineering and law will help to fulfill the requirements of criminal proof standards in socio technical cases.[38]

Burden, Presumptions, and Defenses

Capacity to allocate the burden should be such as to guard the prosecution's onus of proving negligence, knowledge, or recklessness beyond reasonable doubt and, at the same time, create structured defenses which give back to the community honesty and diligence. For example, in a scenario where a certified self-driving feature was activated, a rebuttable presumption could redirect the manner of driving investigation to the authorized entity or licensed operator thereby making the user in charge liable only for certain residual duties. Compliance defenses ought to signal safety cases authenticated, prompt updates, and recall participation, all being recorded under the "Bharatiya Sakshya Adhiniyam, 2023". Investigators may use the audio video recorded seizures under "Section 105" of the BNSS as evidence to contradict the tampering claims. Any dependence on network metadata or V2X packets should be grounded by the "Telecommunications Act, 2023". These adjusted presumption and defenses are the means by which the automation surprise and the misuse which can be foreseen are given their due share. Thus, the residual humans are not unfairly blamed for the mistake, and at the same time, room is preserved to censure the supervisory neglect which is of an outrageous nature.[39]

Policy and Legislative Recommendations

Changes in legislation have the power to change the way the law is practiced on a daily basis. The United Kingdom's 'Automated Vehicles Act 2024'serves as a practical example for authorization, a safe harbor for the user in charge, and offences focusing on the operator. India can incorporate these changes within the BNS and Motor Vehicles structures and still depend on DPDP and BSA for privacy and evidence. PRS Legislative Research has already defined the policy issue by identifying the cross-cutting laws and the lack of a dedicated scheme for the allocation of crimes. The recommendations that follow are a continuation of these threads

[38] David L. Faigman, Joseph Sanders, et.al., *Modern Scientific Evidence: The Law and Science of Expert Testimony* 172 (Thomson West, St. Paul, 1st edn., 2008).
[39] Paul H. Robinson, "A Brief History of Distinctions in Criminal Culpability", 31 *Hastings Law Journal* 815 (1980).

into an India ready road that goes by first defining automated operation, licensing operator entities, clarifying offence allocation by control state, and setting investigation standards that make digital evidence both reliable and proportionate. This route provides a balance between deterrence that is credible and fair attribution in a complicated safety domain.[40]

Amend BNS and MV Act

Targeted amendments should define self-driving operation and the user-in-charge concept within the "Motor Vehicles Act, 1988", then align the "Bharatiya Nyaya Sanhita, 2023" with these definitions for offence allocation. The MV Act should recognize authorized self-driving entities and licensed operators, tie type-approval to safety cases, and integrate recall duties under "Section 110A" with post-market monitoring rules. The BNS should specify that when a certified self-driving feature is engaged, offences for the manner of driving ordinarily attach to the authorized entity or licensed operator, except for explicit residual duties that remain with the user in charge. Linkage clauses should direct courts to use the declared operational design domain and authorization records as objective anchors for control allocation. This pairing gives investigators and courts clear statutory coordinates tied to real control.[41]

Regulatory Sandbox and Type Approval

A national sandbox for AV pilots should run under MV Act rule-making with explicit conditions for route selection, incident reporting, and third-party technical audits. Authorization for self-driving features should require a filed safety case, evidence of verification and validation, driver monitoring thresholds for any residual human roles, and a commitment to in-service monitoring with periodic submissions. When field incidents cross quantitative triggers, recall under "Section 110A" should be activated or updates mandated. Investigative cooperation protocols should incorporate audio-video recorded seizures per "Section 105" of the BNSS and digital-evidence certification under the BSA to ensure downstream admissibility. Transparent summary debriefs will strengthen public trust and supply learning signals without compromising sensitive data, with the DPDP Act providing the lawful processing frame. This

[40] Responsible AI for All – Approach Document, available at: https://www.niti.gov.in/ (last visited on October 25, 2025).
[41] B. M. Gandhi, *Indian Penal Code* 176 (Eastern Book Company, Lucknow, 1st edn., 2017).

approach makes authorization a living safety contract rather than a one-off test.[42]

Data and Telecom Harmonization

Alignment of data and telecommunications law will lead to fewer problems in AV investigations. The DPDP Act defines the processing grounds, rights, and obligations in respect of digital personal data that can be retrieved from event data recorders, cabin cameras, and connected modules. The "Telecommunications Act, 2023" integrates authorization, spectrum, and public safety standards for the networks that carry V2X messages. Regulations should determine the legal bases for investigative access to the logs, retention periods, audit trails, and the secure disclosure to law enforcement and courts. The digital evidence provisions of the BSA should always be the means through which evidence is allowed, thus ensuring that the requirements for chain of custody and certification correspond to the technical aspects. Interfaces that are clearly defined between these statutes will be able to facilitate quick investigations that respect the rights of the individuals in a networked mobility ecosystem where data can be used as evidence and at the same time are sensitive.[43]

Capacity Building

Capacity building must reach police, transport departments, prosecutors, forensic science laboratories, and trial courts. Training should cover control states under SAE J3016, safety case reading, log extraction with audio-video recorded seizures under "Section 105" of the BNSS, and certification pathways under the BSA. Accident investigation teams should learn to correlate vehicle logs with roadside infrastructure, including lawful acquisition of telecom metadata were permitted by the "Telecommunications Act, 2023". Prosecutors and judges need primers on algorithmic decision-making, map-staleness impacts, and take-over dynamics, so that evidentiary weight is assigned to design governance rather than only to human lapses. Over time, a cadre of technical experts accredited for court purposes will reduce uncertainty and accelerate fair outcomes.

[42] Sophia H. Duffy, Jamie Patrick Hopkins, "Sit, Stay, Drive: The Future of Autonomous Car Liability", 16 *SMU Science and Technology Law Review* 453 (2013).
[43] Standing General Order – ADS and ADAS Reporting, available at: https://www.nhtsa.gov/sites/nhtsa.gov/files/2022-06/ADS-SGO-Report-June-2022.pdf (last visited on October 24, 2025).

Conclusion

Indian law on crime is still integrated with aspects that can be used for situations where an automated system is responsible for the crash, but the problem lies in the fact that blame is still being misplaced in cases where real control is elsewhere. Sections 106 and 281 of the Bharatiya Nyaya Sanhita, 2023 are still about negligent killing and rash driving; however, when the ADS performs perception, prediction, and planning, it is often conceptually incorrect to simply connect "manner of driving" liability to a residual human. The duties of the driver to stop, assist, and report (Motor Vehicles Act, 1988, Section 134) and the powers to inspect incident vehicles (Section 136) are vital, as are recall levers (Section 110A read with Rule 127C) for the purpose of remedying system defects. The substrate for evidence is more transparent now: the Bharatiya Sakshya Adhiniyam, 2023 acknowledges electronic and digital records (Sections 61 63), while the BNSS, 2023 requires audio video recording of search and seizure (Section 105), thus securing chain of custody; the lawful handling of personal and in cabin data is governed by the DPDP Act, and V2X traces are under the Telecommunications Act, 2023. In concert, these laws facilitate reconstructing in a probative and rights respecting manner from EDR snapshots, driver monitoring clips, planning logs, and network metadata. Comparative law helps to see the path of principled reallocation: the UK's Automated Vehicles Act 2024 introduces a "user in charge" safe harbor that lessens blame and moves the risk of committing an offence to authorized self-driving entities when the feature is engaged; the AI Act 2024 of the EU and Product Liability Directive 2024 set strict compliance standards and widen the no fault area for software and post-sale updates situations that make knowledge or recklessness of corporate actors more plausible.[44]

The doctrinal center of gravity for criminal negligence in India remains a high threshold that filters ordinary error from gross departures Jacob Mathew, in particular, requires a very cautious approach when criminalizing failure in the complex and expert domains, while Alister Anthony Pareira indicates escalation when intoxication and obvious risks are involved. That viewpoint is also suitable for automation: at Levels 1 2, the human being is still the driver, so red light violations, speeding, intoxication, or post-crash derelictions will be crimes that fall directly under the existing law; at Level 3, where a user is in control, liability for supervisory neglect should be narrowed down (e.g., if an alert was ignored, the person was intoxicated, or

[44] Gary E. Marchant, Rachel A. Lindor, "The Coming Collision Between Autonomous Vehicles and the Liability System", 52 *Santa Clara Law Review* 1321 (2012).

the device was misused), and the "manner of driving" should be considered as coming from an authorized entity if failure modes that were foreseeable had not been mitigated; at Levels 4 5, which are within the ODD, the exposure to offence for system behavior should mostly be connected with the authorized entity/operator and the due diligence defenses should be related to a living safety case and recall cooperation. The impetus for reform is well demonstrated by recent foreign practice. U.S. prosecutors have targeted humans in partial automation cases (e.g., the Uber safety driver probation after a 2018 test crash; the LA case against a Tesla driver using Autopilot) while civil courts and juries have become more critical of corporate understanding and communication (e.g., the 2025 Miami verdict allocating partial fault and imposing $200M punitive damages against Tesla). Adjusting Indian law to include control states, setting up a safe harbor for a user in charge, and licensing operator entities would help culpability to be in line with agency, thus, discouraging unsafe deployment, and maintaining fairness for the remaining humans. All these could be done while using the BSA/BNSS/DPDP/Telecom framework to keep the evidence strong and privacy intact[45].

[45] *Supra* note 50.

Bibliography

Books:

- Andrew Ashworth, *Principles of Criminal Law* (Oxford University Press, Oxford, 1st edn., 2013).
- B. M. Gandhi, *Indian Penal Code* (Eastern Book Company, Lucknow, 1st edn., 2017).
- David L. Faigman, Joseph Sanders, et al., *Modern Scientific Evidence: The Law and Science of Expert Testimony* (Thomson West, St. Paul, 1st edn., 2008).
- Ian Walden, *Computer Crimes and Digital Investigations* (Oxford University Press, Oxford, 1st edn., 2007).
- Jacob Turner, *Robot Rules: Regulating Artificial Intelligence* (Palgrave Macmillan, London, 1st edn., 2019).
- Matthew Channon, Lucy McCormick, et al., *The Law and Autonomous Vehicles* (Routledge, London, 1st edn., 2019).
- Michael I. Krauss, *Principles of Product Liability* (Oxford University Press, Oxford, 1st edn., 2014).
- Peter Cane, Atiyah's Accidents, *Compensation and the Law* (Cambridge University Press, Cambridge, 1st edn., 2013).
- Roger Brownsword, Eloise Scotford, et al., *The Oxford Handbook of Law, Regulation and Technology* (Oxford University Press, Oxford, 1st edn., 2017).
- Ugo Pagallo, *The Laws of Robots: Crimes, Contracts, and Torts* (Springer, Dordrecht, 1st edn., 2013).

Statutes:

- The Automated Vehicles Act, 2024 (United Kingdom Act)

- The Bharatiya Nagarik Suraksha Sanhita, 2023 (Act No. 46 of 2023)
- The Bharatiya Nyaya Sanhita, 2023 (Act No. 45 of 2023)
- The Bharatiya Sakshya Adhiniyam, 2023 (Act No. 47 of 2023)
- The Digital Personal Data Protection Act, 2023 (Act No. 22 of 2023)
- The EU Artificial Intelligence Act, 2024 (European Union Regulation)
- The EU Product Liability Directive, 2024 (Directive (EU) 2024/XXXX)
- The Motor Vehicles Act, 1988 (Act No. 59 of 1988)
- The Telecommunications Act, 2023 (Act No. 44 of 2023)

Articles:

- Bryant Walker Smith, "Automated Vehicles Are Probably Legal in the United States", 1 *Texas A&M Law Review* 411 (2014).
- Dorothy J. Glancy, "Privacy in Autonomous Vehicles", 52 *Santa Clara Law Review* 1171 (2012).
- Eugene Volokh, "Tort Law vs. Privacy", 114 *Columbia Law Review* 879 (2014).
- Gary E. Marchant, Rachel A. Lindor, "The Coming Collision Between Autonomous Vehicles and the Liability System", 52 *Santa Clara Law Review* 1321 (2012).
- Jeffrey K. Gurney, "Sue My Car Not Me: Products Liability and Accidents Involving Autonomous Vehicles", University of Illinois Journal of Law, Technology & Policy 247 (2013).
- Kevin Funkhouser, "Paving the Road Ahead: Autonomous Vehicles, Products Liability, and the Need for a New Approach", 2013 *Utah Law Review* 437 (2013).
- Kyle Graham, "Of Frightened Horses and Autonomous Vehicles: Tort Law and its

Assimilation of Innovations", 52 *Santa Clara Law Review* 1241 (2012).

- Mark A. Geistfeld, "A Roadmap for Autonomous Vehicles: State Tort Law Should Align With Federal Safety Regulations", 105 *California Law Review* 1611 (2017).

- Matthew U. Scherer, "Regulating Artificial Intelligence Systems: Risks, Challenges, Competencies, and Strategies", 29 *Harvard Journal of Law and Technology* 353 (2016).

- Orin S. Kerr, "A User's Guide to the Stored Communications Act, and a Legislator's Guide to Amending It", 72 *George Washington Law Review* 1208 (2004).

- Paul H. Robinson, "A Brief History of Distinctions in Criminal Culpability", 31 *Hastings Law Journal* 815 (1980).

- Sophia H. Duffy, Jamie Patrick Hopkins, "Sit, Stay, Drive: The Future of Autonomous Car Liability", 16 *SMU Science and Technology Law Review* 453 (2013).

- Sven A. Beiker, "Legal Aspects of Autonomous Driving", 52 *Santa Clara Law Review* 1145 (2012).

Websites:

- AI Liability Directive Proposal, *available at:* https://digital-strategy.ec.europa.eu/en/policies/ai-liability-directive (last visited on October 23, 2025).

- Alister Anthony Pareira vs State of Maharashtra on 12 January, 2012, *available at:* https://indiankanoon.org/doc/79026890/ (last visited on October 27, 2025).

- Automated Vehicles Act 2024, *available at:* https://www.legislation.gov.uk/ukpga/2024/10/contents (last visited on October 27, 2025).

- Driver of Tesla on Autopilot Must Stand Trial for Crash that Killed 2 in Gardena, Judge Rules, *available at:* https://abc7.com/post/tesla-gardena-crash-driver/11873142/ (last visited on October 25, 2025).

- Driver of Uber Vehicle Involved in Death of Woman in Tempe Pleads Guilty, *available at:* https://maricopacountyattorney.org/CivicAlerts.aspx?AID=1012 (last visited on

October 19, 2025).

- Jacob Mathew vs State of Punjab & Anr on 5 August, 2005, *available at:* https://indiankanoon.org/doc/871062/ (last visited on October 28, 2025).

- Online High-Definition Map Construction for Autonomous Vehicles: A Comprehensive Survey, *available at:* https://www.mdpi.com/2224-2708/14/1/15 (last visited on October 25, 2025).

- Rafaela Vasquez Pleads Guilty in Fatal Uber Self-Driving Crash That Killed Pedestrian Elaine Herzberg, *available at:* https://www.azcentral.com/story/news/local/tempe/2023/07/28/rafaela-vasquez-pleads-guilty-in-in-fatal-uber-self-driving-crash-killed-pedestrian-elaine-herzberg/70488361007/ (last visited on October 26, 2025).

- Regulation (EU) 2024/1689 Artificial Intelligence Act, *available at:* https://eur-lex.europa.eu/eli/reg/2024/1689/oj/eng (last visited on October 20, 2025).

- Responsible AI for All - Approach Document, *available at:* https://www.niti.gov.in/ (last visited on October 25, 2025).

- SAE J3016 202104, *available at:* https://wiki.unece.org/download/attachments/128418539/SAE%20J3016_202104.pdf (last visited on October 26, 2025).Motor Vehicles Act Resources, available at: https://lawmin.gov.in/ (last visited on October 24, 2025).

- SAE J3016 Taxonomy and Definitions, *available at:* https://www.sae.org/standards/j3016_202104-taxonomy-definitions-terms-related-driving-automation-systems-road-motor-vehicles (last visited on October 28, 2025).

- SAE Levels of Driving Automation, *available at:* https://www.sae.org/news/blog/sae-levels-driving-automation-clarity-refinements (last visited on October 27, 2025).

- Science and Technology Policy Brief: Autonomous Vehicles, *available at:* https://prsindia.org/policy/science-technology-brief/science-technology-policy-brief-autonomous-vehicles (last visited on October 23, 2025).

- Section 110A Recall of Motor Vehicles, *available at:* https://www.indiacode.nic.in/show-data?actid=AC_CEN_30_42_00009_198859_1517807326286&orderno=119&sectionId=50174&sectionno=110A (last visited on October 22, 2025).

- Section 134 Duty of Driver in Case of Accident and Injury to a Person, *available at:* https://www.indiacode.nic.in/show-data?actid=AC_CEN_30_42_00009_198859_1517807326286&orderno=144 (last visited on October 24, 2025).

- Section 136 Inspection of Vehicle Involved in Accident, *available at:* https://indiacode.nic.in/show-data?actid=AC_CEN_30_42_00009_198859_1517807326286&orderno=147 (last visited on October 21, 2025).

- Standing General Order - ADS and ADAS Reporting, *available at:* https://www.nhtsa.gov/sites/nhtsa.gov/files/2022-06/ADS-SGO-Report-June-2022.pdf (last visited on October 24, 2025).

- Tesla Rejected 60 Million Settlement Before Losing 243 Million Autopilot Verdict, *available at:* https://www.reuters.com/legal/litigation/tesla-rejected-60-million-settlement-before-losing-243-million-autopilot-verdict-2025-08-25/ (last visited on October 23, 2025).

- The Bharatiya Sakshya Adhiniyam, 2023, *available at:* https://www.indiacode.nic.in/bitstream/123456789/20063/1/a2023-47.pdf (last visited on October 21, 2025).

- The Digital Personal Data Protection Act, 2023, *available at:* https://www.meity.gov.in/static/uploads/2024/06/2bf1f0e9f04e6fb4f8fef35e82c42aa5.pdf (last visited on October 28, 2025).