



The Indian Journal for Research in Law and Management

Open Access Law Journal – Copyright © 2026

Editor-in-Chief – Dr. Muktai Deb Chavan; Publisher – Alden Vas; ISSN: 2583-9896

This is an Open Access article distributed under the terms of the Creative Commons Attribution-Non-Commercial-Share Alike 4.0 International (CC-BY-NC-SA 4.0) License, which permits unrestricted non-commercial use, distribution, and reproduction in any medium provided the original work is properly cited.

CYBERSECURITY LIABILITY IN AUTONOMOUS VEHICLES: RETHINKING PRODUCT LIABILITY IN THE AGE OF CYBER- PHYSICAL HARM

~ Ryan Bang, Ankit Singh & Deepika Mohnani

Abstract

The transition from mechanically operated automobiles to software-defined and increasingly autonomous vehicles unsettles the conceptual foundations of product liability. A conventional product defect is ordinarily understood as a condition existing when a product leaves the manufacturer's control; cybersecurity vulnerabilities, by contrast, may emerge after deployment, remain latent until exploited, propagate across an entire vehicle fleet, and transform a digital weakness into bodily, proprietary, or economic harm. The resulting liability problem is therefore not merely one of defective driving technology, but of allocating responsibility where software, manufacturers, suppliers, vehicle owners, regulators, and malicious third parties intersect.

This paper examines whether existing liability frameworks are capable of addressing such cyber-physical harm, through a comparative analysis of the European Union, the United States, and India. It argues that the European model presently offers the most conceptually coherent architecture by combining the preventive obligations of UN Regulation No. 155 with the emerging strict-liability framework of the 2024 Product Liability Directive, including its express treatment of software, cybersecurity vulnerabilities, post-market updates, evidentiary disclosure, and third-party attacks. The United States, by contrast, continues to rely principally upon state tort law, recalls, and non-binding cybersecurity guidance, leaving significant questions of defect, foreseeability, standing, economic loss, and proof unresolved. India occupies a more consequential regulatory gap: while

section 164 of the Motor Vehicles Act, 1988 provides a limited no-fault compensation floor and proposed Rules 125-T and 125-U would introduce cybersecurity and software-update requirements, its existing product-liability framework does not adequately accommodate software defects, non-consumer victims, or malicious third-party interference.

The paper consequently argues for an Indian framework that connects ex ante cybersecurity compliance with ex post civil liability. It proposes recognition of cybersecurity vulnerabilities and safety-critical failures to update as actionable product defects, disclosure and evidentiary presumptions for technologically asymmetric litigation, manufacturer responsibility notwithstanding third-party attacks, expanded standing for persons injured by compromised vehicles, and a collective compensation mechanism for correlated or fleet-wide cyberattacks. The central claim is that cybersecurity liability cannot be resolved by treating the autonomous vehicle as merely another defective product: the law must account for the vehicle as a continuously evolving cyber-physical system whose safety obligations persist beyond the moment of sale.

I. Introduction

The automobile was once principally a mechanical product, and product-liability law developed accordingly. Defective brakes, steering systems, or manufacturing components could be traced to a relatively identifiable point of failure and assessed through established doctrines of defect, causation, and negligence. Connected and autonomous vehicles disrupt this legal simplicity. Their safety increasingly depends upon software that is continuously updated, remotely connected, and susceptible to deliberate interference. A vulnerability may therefore emerge after sale, remain dormant until exploited, and convert a digital weakness into physical injury. The resulting harm is distinctly cyber-physical: the means of interference is digital, but the consequence may be bodily, proprietary, or economic.

The difficulty is compounded by the presence of a malicious third party between the manufacturer and the ultimate harm. Responsibility may implicate the vehicle manufacturer, software developer, component supplier, vehicle owner, or attacker, while the evidence necessary to establish causation—source code, forensic logs, security assessments and update records—often remains

under the manufacturer's control. Traditional doctrines of product liability and negligence consequently struggle with questions of defect, foreseeability, proof, and economic loss.

This paper examines that liability problem comparatively through the legal frameworks of the European Union, the United States, and India. It argues that while the European framework has moved towards integrating cybersecurity regulation with product liability, the United States continues to rely substantially upon tort law and recall mechanisms, and India remains without a dedicated regime despite emerging cybersecurity requirements for vehicles. The paper ultimately proposes an Indian framework that connects preventive cybersecurity obligations with post-harm liability by recognising cybersecurity vulnerabilities as product defects, improving access to technical evidence, addressing third-party attacks, and extending protection to persons injured by compromised vehicles.

II. Cybersecurity Liability in AVs

A. From Mechanical Defect to Cyber-Physical Harm

Modern product liability grew out of mechanical failure. In *MacPherson v Buick Motor Co* a purchaser injured when a wheel collapsed was allowed to sue the manufacturer with whom he had no contract.¹ *Donoghue v Stevenson* reached a similar place in England through a duty of care owed to the ultimate consumer,² and California later adopted strict liability in tort for defective products.³ The Restatement (Third) of Torts sorts product defects into manufacturing defects, design defects and inadequate warnings.⁴ Each category presumes a defect that was present when the product left the manufacturer, and a wheel is either sound or it is not.

Software unsettles that presumption in three ways. It is never finished, because it is patched for as long as the vehicle is used. It is connected, so a weakness in one component can be reached from outside the vehicle. And it can fail because someone deliberately makes it fail. The UN Regulation on vehicle cybersecurity defines cyber security as the condition in which road vehicles and their

¹ *MacPherson v Buick Motor Co* 217 NY 382 (1916).

² *Donoghue v Stevenson* [1932] AC 562 (HL).

³ *Greenman v Yuba Power Products Inc* 59 Cal 2d 57 (1963).

⁴ Restatement (Third) of Torts: Products Liability (American Law Institute 1998) s 2.

functions are protected from cyber threats to electrical or electronic components.⁵ The harm that follows is cyber-physical: the means is digital and the injury is bodily or proprietary. In an autonomous vehicle the sensors, decision software and actuators that replace the driver are themselves the surface to be attacked.

B. The Jeep Cherokee Hack and the Rise of Automotive Cybersecurity Law

The risk became concrete in July 2015, when the researchers Charlie Miller and Chris Valasek took remote control of a Jeep Cherokee that a *Wired* journalist was driving on a highway, reaching its brakes, steering and transmission through the cellular-connected infotainment system.⁶ Within days Fiat Chrysler announced a recall of about 1.4 million vehicles in the United States to install a software fix, which has been described as the first recall prompted by a cyber vulnerability alone.⁷ No driverless car was involved. The Seventh Circuit later recorded that, apart from the vehicle in the magazine's test, no other Chrysler vehicle was successfully hacked.⁸ The episode matters for another reason. A weakness in a system designed by one company, Harman, and fitted by another, FCA, could be reached remotely, and the only regulatory tool at hand was the recall process built for brake and airbag defects.

Litigation did not help those who tried to sue over the risk. In *Cahen v Toyota Motor Corp* owners of vehicles said to be hackable were held to lack standing.⁹ Regulators moved by guidance first. The National Highway Traffic Safety Administration (NHTSA) issued cybersecurity best practices in 2016 and updated them as voluntary guidance in 2022,¹⁰ and UN Regulation No 155 entered into force on 22 January 2021, making cybersecurity a condition of vehicle type approval.¹¹ Automotive cybersecurity law thus began with a demonstration, passed through recalls and guidance, and took binding form about six years later, and then only on the preventive side. Nothing in it says who pays when prevention fails.

⁵ UN Regulation No 155 ('UN R155'), para 2.2, consolidated text at [2025] OJ L 2025/5.

⁶ Andy Greenberg, 'Hackers Remotely Kill a Jeep on the Highway, With Me in It' *Wired* (21 July 2015).

⁷ Associated Press, 'Fiat Chrysler recalls 1.4M vehicles to prevent hacking' (24 July 2015); Design News, 'Jeep Hack Sparks Massive Recall from Chrysler' (27 July 2015).

⁸ *Flynn v FCA US LLC* (7th Cir, No 20-1698, 14 July 2022); class certification is reported at 327 FRD 206 (SD Ill 2018).

⁹ *Cahen v Toyota Motor Corp* 147 F Supp 3d 955 (ND Cal 2015), affirmed 717 F App'x 720 (9th Cir 2017).

¹⁰ NHTSA, *Cybersecurity Best Practices for the Safety of Modern Vehicles* (September 2022), updating the 2016 edition.

¹¹ UN R155, ECE/TRANS/WP.29/2020/79 as amended (entry into force 22 January 2021).

C. Why Product Liability and Negligence Struggle with Cyberattack Harm

Four difficulties recur. The first is defect. A risk-utility approach asks whether a precaution of tolerable cost would have prevented the harm, which is the reasoning of the Learned Hand formula weighing the burden of precaution against the probability and gravity of loss.¹² Applied to software the test has no natural stopping point. Large code bases contain vulnerabilities, so the existence of a flaw cannot itself be the defect, and the question becomes how much security effort was enough, on which neither courts nor statutes supply a benchmark.

The second is the attacker. The deliberate criminal act of a third party is ordinarily a superseding cause unless the defendant should have realised the likelihood of such conduct.¹³ After 2015 the foreseeability of attack in general is hard to deny, but the doctrine still invites argument over which attack, through which interface, was foreseeable.

The third is proof. The evidence of how a vehicle was compromised lies in logs, source code and back-end servers that the manufacturer controls, and a bystander has no means of reaching it. A RAND study of hacked autonomous vehicles found existing civil liability flexible enough for most claims, large-scale attacks being the exception.¹⁴ That finding presupposes a claimant able to plead and prove a theory, which is the point in doubt.

The fourth is loss. Where a flaw is found and patched before anyone is hurt, the owners' loss is economic, and tort systems resist recovery for economic loss caused by a defective product.¹⁵ Federal courts add a threshold rule that future injury must be certainly impending.¹⁶ The cases easiest to prove, in which a hack has injured someone, are rare, and the cases most likely to arise, in which a vulnerability exists, are the hardest to bring.

D. Cybersecurity Liability vs Ordinary AV Crash Liability

Writing on automated vehicles has mostly addressed crashes caused by the driving system. Abraham and Rabin propose that manufacturers answer for injuries arising from the operation of

¹² *United States v Carroll Towing Co* 159 F 2d 169 (2d Cir 1947).

¹³ Restatement (Second) of Torts (American Law Institute 1965) ss 448-449.

¹⁴ Zev Winkelman and others, *When Autonomous Vehicles Are Hacked, Who Is Liable?* (RAND Corporation 2019).

¹⁵ *East River Steamship Corp v Transamerica Delaval Inc* 476 US 858 (1986).

¹⁶ *Clapper v Amnesty International USA* 568 US 398 (2013).

highly automated vehicles, replacing driver negligence with manufacturer responsibility,¹⁷ and Smith has examined how product liability would apply to automated driving.¹⁸ There the chain runs from the vehicle's own failure of perception or planning to the injury, and the manufacturer is the natural defendant because it designed the failing system.

A cyberattack differs in four respects. A human adversary stands between design and harm. The fault may lie in the security architecture, in a supplier's component, in a late patch or in an owner who refused an update, so responsibility is shared. The risk is correlated: one exploited flaw can reach every vehicle running the same software build, which is why Channon and Marson argue that cybersecurity liability calls for its own strategy.¹⁹ And the duty runs past the sale, because a manufacturer can reduce the risk after delivery only by monitoring and updating. A rule that attributes an accident to the vehicle's driving decisions answers none of these points.

III. The European Union Framework

A. UN R155 and the CSMS as a Type-Approval Precondition

UN Regulation No 155 applies to vehicles of categories L, M, N and O that are fitted with at least one electronic control unit,²⁰ a scope wide enough to take in ordinary connected cars as well as automated ones. Its centre is the Cyber Security Management System (CSMS), a systematic risk-based approach to organisational processes, responsibilities and governance. The manufacturer must show that the system covers development, production and post-production, and monitoring must continue for vehicles after first registration, including the capacity to analyse threats, vulnerabilities and attacks from vehicle data and logs.²¹ The post-production duty is the one that matters most for liability.

Compliance has two layers. The manufacturer needs a valid certificate of compliance for its CSMS, issued for at most three years,²² and each vehicle type must then be approved. For the type the

¹⁷ Kenneth S Abraham and Robert L Rabin, 'Automated Vehicles and Manufacturer Responsibility for Accidents: A New Legal Regime for a New Era' (2019) 105 Virginia Law Review 127.

¹⁸ Bryant Walker Smith, 'Automated Driving and Product Liability' [2017] Michigan State Law Review 1.

¹⁹ Matthew Channon and James Marson, 'The Liability for Cybersecurity Breaches of Connected and Autonomous Vehicles' (2021) 43 Computer Law & Security Review.

²⁰ UN R155, para 1.1.

²¹ UN R155, paras 2.3, 7.2.2.1 and 7.2.2.4.

²² UN R155, paras 6.7 and 7.3.1.

manufacturer must identify critical elements, carry out an exhaustive risk assessment against the threats listed in Annex 5, implement proportionate mitigations, test them before approval and provide the data forensic capability needed to analyse attempted or successful attacks.²³ It must also report on its monitoring to the approval authority at least once a year.²⁴

In the Union the regulation binds through Regulation (EU) 2019/2144, to which a delegated regulation of 2022 added UN R155.²⁵ It applied to new vehicle types from July 2022 and to all new vehicles from July 2024, and a companion regulation, UN R156, deals with software update management.²⁶ The Cyber Resilience Act excludes products covered by Regulation 2019/2144, so vehicles stay on the type-approval route.²⁷ R155 is a compliance regime. It prescribes processes and evidence, and says nothing about who compensates a person injured despite them.

B. The Product Liability Directive 2024/2853: Software and Cybersecurity as Defects

Directive (EU) 2024/2853 was adopted on 23 October 2024 and replaces Directive 85/374/EEC. Member States must bring it into force by 9 December 2026, and it applies to products placed on the market or put into service after 8 December 2026, a date that a corrigendum of May 2026 substituted for the originally published 9 December.²⁸ Earlier products remain under the old directive.

Three features matter for vehicles. First, software is a product. The definition covers all movables, even when integrated into or interconnected with another movable, and expressly includes software, and the recitals treat the developer of software as a manufacturer.²⁹ The vehicle manufacturer is liable, and so, jointly and severally, is the manufacturer of a defective component integrated within its control, a category that takes in software updates and related digital services.³⁰ Secondly, defect is measured by the safety a person is entitled to expect, taking into account among

²³ UN R155, paras 5.1.1, 5.1.2, 7.3.3 to 7.3.7 and Annex 5.

²⁴ UN R155, para 7.4.1.

²⁵ Commission Delegated Regulation (EU) 2022/1398 of 8 June 2022 amending Regulation (EU) 2019/2144, annexes I and II.

²⁶ Vehicle Certification Agency (UK), 'Cyber Security and Software Updating' (14 May 2024) (setting out the dates of application and describing UN R156).

²⁷ Regulation (EU) 2024/2847 (Cyber Resilience Act), art 2(2)(c).

²⁸ Directive (EU) 2024/2853 on liability for defective products [2024] OJ L 2024/2853 ('PLD'), arts 2(1), 21 and 22(1), as corrected by Corrigendum [2026] OJ L 2026/90364 (7 May 2026).

²⁹ PLD, arts 4(1) and 4(10)(a); recital 13.

³⁰ PLD, arts 4(4)-(5), 8(1)(b) and 12(1); recitals 17-19.

other things any ability of the product to learn or acquire new features after sale, the moment the product left the manufacturer's control, and relevant product safety requirements, including safety-relevant cybersecurity requirements.³¹ The recitals add that a product may be found defective on account of a cybersecurity vulnerability. Thirdly, the directive narrows the usual exits. A manufacturer cannot say that a defect arose after the product was placed on the market where it is due to software, including updates, or to a lack of updates necessary to maintain safety, provided these are within its control.³² The recitals tie this to cybersecurity vulnerabilities, while stating that the directive imposes no obligation to supply updates and that liability does not arise where an owner fails to install an update that was supplied.³³ For attacks, the key rule is that an economic operator's liability is not reduced because a third party also contributed to the damage; the recitals give the example of a third party exploiting a vulnerability. Liability may be reduced for the injured person's own fault.³⁴

The claimant must still prove defect, damage and causation, with help. Courts may order disclosure of relevant evidence. Defect is presumed if the defendant fails to disclose, or if the product breaches mandatory safety requirements aimed at the damage suffered. Defect or causation is presumed where technical complexity makes proof excessively difficult and the claimant shows likelihood.³⁵ Compensation covers death, personal injury, damage to property not used exclusively for professional purposes, and destruction or corruption of data not used for professional purposes.³⁶

C. Ex-Ante Regulation and Ex-Post Liability Interaction

The two instruments are not formally joined, but the directive draws on type-approval law at several points. Safety-relevant cybersecurity requirements count in assessing defect, breach of a mandatory safety requirement raises a presumption of defect, and a recall or similar intervention may be taken into account, though the recitals say it does not itself create a presumption.³⁷ Compliance with R155 does not protect a manufacturer, since the compliance defence applies only

³¹ PLD, art 7(1)-(2); recital 32.

³² PLD, art 11(2).

³³ PLD, recital 51.

³⁴ PLD, art 13; recital 55.

³⁵ PLD, arts 9 and 10(2)-(4).

³⁶ PLD, art 6(1).

³⁷ PLD, arts 7(2)(f)-(g), 10(2)(b) and 11(1)(d); recital 34.

where the defect is due to compliance. Evidence is a second point of contact. R155 obliges manufacturers to hold forensic data and to monitor vehicles in service, and that material is what a claimant would seek under the disclosure rule. The Court of Justice has already shown how it reads defect and proof in the older directive. A product can be found defective because of a defect in other items of the same production series,³⁸ and national courts may rely on serious, specific and consistent evidence to find causation where scientific proof is unavailable.³⁹

D. Coherence and Limitations of the EU Model

The model is coherent in that the preventive and compensatory rules point the same way: the vehicle must be built and monitored to a standard, and a failure to keep it secure counts against the manufacturer when someone is hurt. Its limits are practical. The directive reaches only products placed on the market after December 2026, expiry runs ten years from placement, and compensation is for natural persons, which excludes a fleet operator's professionally used property and pure economic loss.⁴⁰ There is no duty to supply updates, so a manufacturer that stops patching a model risks liability but breaches nothing. Nothing addresses a mass attack whose damages exceed what manufacturers can pay; compensation schemes for insolvent operators are permitted, not required. The proposed AI Liability Directive, meant to ease fault-based claims involving artificial intelligence, was withdrawn, with notice published in the Official Journal on 6 October 2025.⁴¹ And since the directive has yet to apply to any vehicle, no court has interpreted its cybersecurity provisions, so the claim of coherence rests on design and not on experience.

IV. The United States Framework

A. Absent Federal Legislation: SELF DRIVE Act to H.R. 7390

The United States has no federal statute on automated driving systems and none that allocates liability for their cybersecurity. The SELF DRIVE Act of 2017 cleared the House of

³⁸ Joined Cases C-503/13 and C-504/13 *Boston Scientific Medical Device* EU:C:2015:148; see PLD, recital 30.

³⁹ Case C-621/15 *NW v Sanofi Pasteur MSD* EU:C:2017:484.

⁴⁰ PLD, arts 5(1), 6(1)(b)(iii), 8(5) and 17(1).

⁴¹ Commission notice withdrawing the proposal for a directive on adapting non-contractual civil liability rules to artificial intelligence, COM(2022) 496, published 6 October 2025 (EUR-Lex procedure 2022/0303/COD).

Representatives but did not become law,⁴² and the name has now been given to H.R. 7390, introduced by Representative Latta on 5 February 2026.⁴³

The 2026 bill shows what Congress is prepared to do. A manufacturer would have to develop a safety case before selling an automated driving system or an ADS-equipped vehicle, and the competencies the case must cover include a cybersecurity plan: a written policy on detecting and responding to attacks and false vehicle control commands, a process to identify, assess and mitigate reasonably foreseeable cyber risks, and a process for preventive and corrective action, including incident response and intrusion detection.⁴⁴ The plan is a document to be produced and not a standard to be met, and the bill contains no rule on compensation. It provides that compliance with the safety case provisions does not exempt anyone from liability at common law, so tort law would carry on. A separate section directs the Commerce Department to review its connected vehicle supply chain rule,⁴⁵ which concerns national security and not injury.

Progress has been slow. A House subcommittee forwarded the bill on 10 February 2026 by 12 votes to 11,⁴⁶ and by mid-June the full Energy and Commerce Committee had not reached consensus, although its leadership intended to pursue the bill as part of a surface transportation package.⁴⁷ On the material available at the time of writing, nothing enacted sets a federal cybersecurity standard for automated vehicles.

B. NHTSA's Role: SGO, FMVSS Reform and AV STEP

NHTSA acts under the National Traffic and Motor Vehicle Safety Act. It can prescribe Federal Motor Vehicle Safety Standards and can require manufacturers to remedy safety-related defects by recall.⁴⁸ There is no standard on vehicle cybersecurity. There is guidance: the agency's 2022 best

⁴² SELF DRIVE Act of 2017, HR 3388, 115th Cong; Repairer Driven News, 'Congress subcommittee shows wide favor of SELF DRIVE Act, some safety criticisms cited' (13 February 2026) (remarks of Rep Debbie Dingell on the 2017 bill).

⁴³ SELF DRIVE Act of 2026, HR 7390, 119th Cong (introduced 5 February 2026).

⁴⁴ HR 7390, s 3, proposed 49 USC s 30130(b)(3)-(4), including para (4)(H); the common-law savings language is in the preemption provision of the same section.

⁴⁵ HR 7390, s 6; Securing the Information and Communications Technology and Services Supply Chain: Connected Vehicles, 90 Fed Reg 5360 (2025).

⁴⁶ House Committee on Energy and Commerce, 'CMT Subcommittee Forwards Motor Vehicle Safety and Automotive Leadership Bills to Full Committee' (10 February 2026).

⁴⁷ Holland & Knight, 'House Passes Autonomous Vehicles Framework for Commercial Motor Vehicles' (17 June 2026) (also describing the BUILD America 250 Act, HR 8870).

⁴⁸ 49 USC ss 30111, 30118-30120.

practices are non-binding, recommend the NIST framework and secure software development, and point to the ISO/SAE 21434 engineering standard.⁴⁹ The recall power has nonetheless been used for cybersecurity, as the 2015 Fiat Chrysler recall showed.

NHTSA's recent work on automated driving has concentrated on reporting and exemptions. Standing General Order 2021-01 requires crash reporting for vehicles with automated driving systems and certain driver assistance systems, and it was streamlined in 2025 to remove requirements the agency regarded as unnecessary or duplicative. Under the Department of Transportation's AV Framework of April 2025 the agency also widened its exemption programme to vehicles built in the United States and simplified general exemptions. The standards were written for vehicles with a human driver, which is why exemptions carry much of the load for novel designs.⁵⁰ None of this concerns cybersecurity.

AV STEP needs separate treatment. NHTSA proposed it on 15 January 2025 as a voluntary framework in which participants would submit independent assessments of their safety cases and report operational data.⁵¹ The proposal has since been withdrawn. A notice published on 26 June 2026 records that industry thought the burden outweighed the benefit of a voluntary scheme, that safety advocates thought it gave too little oversight, and that some of its aims had been met by other initiatives.⁵² The one federal programme designed to examine safety cases is therefore no longer proposed, and the federal government is left with recalls, exemptions and crash data.

C. State Tort Law as the Default Mechanism

With no federal rule, liability is a matter of state law, and states apply the ordinary categories of manufacturing defect, design defect and failure to warn⁵³ to a new subject. The record on cybersecurity claims is thin. In *Cahen* the court dismissed for want of standing the claims of owners whose complaint was that their vehicles could be hacked, and the Ninth Circuit affirmed.

⁴⁹ Alston & Bird, 'NHTSA Updates Its Guidance on Cybersecurity Best Practices for the Safety of Modern Vehicles' (Privacy, Cyber & Data Strategy Blog, September 2022).

⁵⁰ ADS-Equipped Vehicle Safety, Transparency, and Evaluation Program; Withdrawal, FR Doc 2026-12980 (published 26 June 2026) (describing changes to Standing General Order 2021-01 and to the exemption programmes under 49 USC ss 30113 and 30114).

⁵¹ ADS-Equipped Vehicle Safety, Transparency, and Evaluation Program (notice of proposed rulemaking) 90 Fed Reg 4130 (15 January 2025).

⁵² ADS-Equipped Vehicle Safety, Transparency, and Evaluation Program; Withdrawal, FR Doc 2026-12980, parts II and III.

⁵³ Restatement (Third) of Torts: Products Liability ss 1-2.

In *Flynn*, the Jeep litigation, plaintiffs survived the pleadings on an overpayment theory, but the district court dismissed after discovery because they had produced no evidence of that injury, and the Seventh Circuit agreed in 2022.⁵⁴ Neither court reached the merits of a design-defect claim.

The nearest success for plaintiffs concerns driver assistance and not hacking. In August 2025 a federal jury in Miami found Tesla 33 per cent responsible for a fatal crash involving Autopilot and awarded punitive damages of 200 million dollars, and the trial judge later declined to set the verdict aside.⁵⁵ It shows that juries will hold a manufacturer liable for a software-driven system. The plaintiffs' case, however, was about how the system was designed and marketed, and no third-party attack was in issue.

D. Adequacy of a Litigation-Driven Approach

Leaving the standard of care to be formed case by case has costs for a risk of this kind. The standard arrives late, after injuries, and reflects the facts of one dispute and not an assessment of the technology. Standing and economic-loss rules keep the large class of unexploited vulnerabilities out of court, so recalls and voluntary standards do most of the preventive work. A federal bill that displaces some state deployment rules but preserves common-law liability, while requiring only a cybersecurity plan, would leave the question of who pays where it now stands, and would make the courts more important and not less. American law shows how much tort and recall can achieve, and also where they stop.

V. The Indian Framework and the Need for Reform

A. Absence of a Dedicated AV Cybersecurity Liability Regime

India has no statute on autonomous vehicles and no provision on liability for their cybersecurity. The Motor Vehicles Act, 1988 assumes a human driver: no person may drive a motor vehicle in a public place without an effective driving licence,⁵⁶ and its compensation provisions are built around the owner and the insurer. Policy is also against driverless vehicles. The Union Minister

⁵⁴ *Cahen v Toyota Motor Corp* 147 F Supp 3d 955 (ND Cal 2015); *Flynn v FCA US LLC* (7th Cir, No 20-1698, 14 July 2022).

⁵⁵ *Benavides v Tesla Inc* (SD Fla, jury verdict 1 August 2025); Reuters, 'Judge upholds \$243M verdict against Tesla over fatal Autopilot crash' (Business Insurance, February 2026).

⁵⁶ Motor Vehicles Act 1988, s 3(1).

for Road Transport and Highways said in September 2025 that driverless cars would not be permitted because of their effect on drivers' employment.⁵⁷

The statute leaves a door ajar. The 2019 amendment inserted section 2B, which lets the Central Government, to promote innovation, research and development in vehicular engineering, exempt certain types of mechanically propelled vehicles from the Act.⁵⁸ Whether it will be used for automated driving is unknown. In the near term the live question is not driverless cars at all. It is conventional vehicles with growing software content, driver assistance and over-the-air updates and, at the upper end, vehicles with conditional automation in which a human remains available as fallback, the levels being those of SAE J3016.⁵⁹ Those vehicles raise the liability problem in full while staying inside the policy line. For them the law that applies is the general law.

B. MV Act, Consumer Protection Act, and IT Act: Applicability and Gaps

The Motor Vehicles Act. A person killed or seriously hurt in an accident arising out of the use of a motor vehicle has a no-fault claim under section 164: five lakh rupees to the legal heirs on death and two and a half lakh rupees to the victim for grievous hurt, payable by the owner or the authorised insurer without proof of any wrongful act, neglect or default.⁶⁰ The section replaced the earlier no-fault provisions from 1 April 2022, and the Supreme Court has applied it to enhance awards.⁶¹ For a victim of a hacked vehicle it is a floor that is quick and indifferent to cause. It does not touch the manufacturer, and the sums are modest. Anything above the floor needs a fault-based claim, which needs someone at fault. Section 110A, inserted in 2019, allows the Central Government to order a manufacturer to recall vehicles where a defect may harm the driver, occupants or other road users, on reports from owners, a testing agency or any other source.⁶² Whether a software vulnerability is a 'defect' for the section is untested, though the wording would bear that reading.

⁵⁷ 'Transport Minister Nitin Gadkari Says He Won't Allow Driverless Cars In India: Explains Why' (CarToq, 9 September 2025) (reporting remarks at the FICCI Road Safety Awards and Symposium).

⁵⁸ Motor Vehicles (Amendment) Act 2019 (Act 32 of 2019), s 3, inserting s 2B.

⁵⁹ SAE International, *Taxonomy and Definitions for Terms Related to Driving Automation Systems for On-Road Motor Vehicles* (J3016, April 2021 edition).

⁶⁰ Motor Vehicles Act 1988, s 164.

⁶¹ *Ram Murti v Punjab State Electricity Board* (SC, Civil Appeal No 7143 of 2022, 11 October 2022); LiveLaw, 'Motor Vehicles Act: New Provisions On Third Party Insurance, Accident Claims To Come Into Effect From April 1, 2022' (February 2022).

⁶² Motor Vehicles Act 1988, s 110A.

The Consumer Protection Act, 2019. Chapter VI makes a product manufacturer liable for harm caused by a defective product, frames liability through manufacturing and design defects, departure from specifications, breach of express warranty and inadequate instructions, and defines ‘defect’ by reference to faults in quality or standard required by law or contract.⁶³ Four gaps follow. ‘Product’ is defined in terms of articles, goods, substances and raw materials, with no reference to software or digital services, so a claim founded on a flawed update must argue that software is part of the goods. ‘Harm’ excludes harm to the product itself and commercial or economic loss,⁶⁴ which shuts out the owner whose vehicle is disabled. Standing is tied to the consumer, who is a buyer or a user with the buyer’s approval,⁶⁵ so a pedestrian struck by a compromised vehicle falls outside the complainant categories. And nothing says how a third party’s attack bears on the manufacturer’s liability.

The Information Technology Act, 2000. Section 43 makes a person who without permission accesses a computer, introduces a virus or disrupts a computer system liable to compensate the person affected, with claims up to five crore rupees going to an adjudicating officer.⁶⁶ The provision is aimed at the attacker, the party least likely to be found or to pay, and it does not address a manufacturer’s failure to secure the system. The CERT-In directions of 28 April 2022 require reporting of listed incidents, including attacks on Internet of Things devices, within six hours.⁶⁷ That informs the government and gives victims no right.

C. Draft Rules 125-T/125-U and AIS-189/190: Scope and Limitations

A draft notification dated 22 June 2026 proposes to insert Rules 125-T and 125-U in the Central Motor Vehicles Rules, 1989. Rule 125-T would require vehicles of categories M, N and T fitted with at least one electronic control unit, and L7 vehicles with Level 3 automation, to meet AIS-189 on cybersecurity and cybersecurity management systems. Vehicles with Level 3 automation or above face the first deadlines, 1 October 2026 for new models and 1 April 2027 for existing ones, with later deadlines for other vehicles running to 2029, and comments were invited for thirty

⁶³ Consumer Protection Act 2019, ss 2(10), 2(33)-(34), 82-84 and 87.

⁶⁴ Consumer Protection Act 2019, s 2(22).

⁶⁵ Consumer Protection Act 2019, ss 2(5) and 2(7).

⁶⁶ Information Technology Act 2000, ss 43 and 46(1A).

⁶⁷ CERT-In, Directions under sub-section (6) of section 70B of the Information Technology Act 2000 (28 April 2022).

days.⁶⁸ Rule 125-U would require compliance with AIS-190 on software update management for a wider group of categories, M, N, T, A and C, and both standards would stay in force until the Bureau of Indian Standards notifies corresponding specifications.⁶⁹ No notification of final rules has come to the author's notice.

The design follows the United Nations model, and the draft has been presented as aligning India with international practice. Its limits are those of R155. It is a type-approval and compliance scheme: a manufacturer that fails the standard cannot obtain approval. The reports of the draft say nothing about compensation, about evidence, or about what follows when a certified vehicle is hacked. Approval depends on testing agencies recognised under the Act,⁷⁰ and whether they can audit management systems and test vehicles against threat lists of the Annex 5 type is a practical question the draft cannot answer. Even if finalised unchanged, the draft improves prevention and leaves the post-harm question where it was.

D. India-Specific Constraints: Roads, Policy Stance, Regulatory Capacity

Three conditions shape what India can borrow. The first is the road environment: mixed traffic and inconsistent road markings are generally regarded as obstacles to high levels of automation. The second is the employment stance, which means regulation will be framed around conventional vehicles with advanced software and not around driverless ones. That is a reason to act now, since the draft rules already reach every new connected vehicle with an electronic control unit. The third is regulatory capacity. Approval rests on designated testing agencies, and the Consumer Protection Act has no disclosure or presumption mechanism comparable to Articles 9 and 10 of the Union directive. Capacity limits favour a regime that adds few institutions, relies on certification evidence manufacturers must already keep, and uses the recall power that exists.

VI. Comparative Analysis and Recommendations

⁶⁸ PTI, 'MoRTH Proposes Phased Rollout of Cybersecurity Management Systems for Vehicles' (Outlook Business, 27 June 2026) (reporting a draft notification dated 22 June 2026).

⁶⁹ 'India proposes mandatory cybersecurity rules for connected vehicles' (AutoGuide India, 2026).

⁷⁰ Motor Vehicles Act 1988, ss 2(42A) and 110B.

A. Comparative Assessment of the Three Jurisdictions

Side by side, the three systems differ on both halves of the problem. On prevention the Union has binding rules in force: new vehicles may not in general be registered without type approval to R155.⁷¹ The United States has guidance and a pending bill that would add a cybersecurity plan to a safety case. India has a draft. On compensation the Union will from December 2026 apply a strict-liability regime that treats software and missing security updates as sources of defect, leaves the manufacturer liable when a third party's attack contributes to the harm, and gives claimants disclosure and presumptions. The United States relies on state tort law, whose cybersecurity record is one of cases lost at the threshold. India has a no-fault floor in the Motor Vehicles Act and a consumer statute that was not drafted with software or bystanders in mind.

The hypothesis is borne out, with two qualifications. The European model is the more coherent on paper, because its two instruments share concepts and evidence, but it has not yet been applied, and coherence is not performance; American juries have already returned real verdicts against manufacturers in driver-assistance cases. The Indian position is also better than the hypothesis allows in one respect: section 164 means a victim does not go away empty-handed. The gap lies above that floor, where the manufacturer's liability must be established, and there the Consumer Protection Act is poorly equipped.

B. Elements Transferable to India

Four elements travel well. The first is the statutory statement that a vulnerability, or a failure to supply a security update necessary for safety, can make a product defective, together with the rule that a defect arising later is no answer where its cause lies within the manufacturer's control. It turns an open question in tort into a rule. The second is the evidence package of disclosure and rebuttable presumptions, which suits systems whose code the claimant cannot see. The third is the allocation under which a third party's attack does not reduce the manufacturer's liability, paired with a reduction for an owner who ignores an update. The fourth is to use the forensic logging that R155 already demands as the bridge between regulation and claims. The American lesson is a negative one. Leaving cybersecurity to tort and recall means that unexploited vulnerabilities never reach a court, so India's recall power under section 110A should be tied expressly to software

⁷¹ UN R155, para 7.3.1 (transitional allowance for certain type approvals issued before 1 July 2024); Commission Delegated Regulation (EU) 2022/1398 of 8 June 2022.

vulnerabilities. Two things do not travel: the ten-year expiry period, which would need adapting to the working life of a vehicle, and reliance on national courts with developed disclosure practice. Section 164 supplies something the Union directive does not and should stay as the baseline.

C. Recommendations for an Indian Regulatory Framework

Five measures follow. First, Rules 125-T and 125-U should be finalised, with an added duty on manufacturers to retain the forensic and monitoring data on which compliance rests, for a defined period, and to produce it on lawful request.

Second, the Consumer Protection Act, 2019 should be amended so that ‘product’ includes software and digital services integrated into or interconnected with a vehicle and within the manufacturer’s control; so that a security vulnerability, and a failure to supply a security update necessary to maintain safety, may be a defect; and so that a third party’s attack does not reduce the manufacturer’s liability, while an owner’s unreasonable failure to install a supplied update may reduce the owner’s recovery.

Third, those proceedings need an evidence rule: disclosure of relevant material by the manufacturer on a plausible claim, and a rebuttable presumption of defect where the vehicle does not meet a mandatory requirement under the Central Motor Vehicles Rules or the manufacturer fails to disclose.

Fourth, the right to sue under the product liability chapter should extend to persons injured by the vehicle who are not consumers, so that a pedestrian or another driver stands where the owner stands.

Fifth, for harm that cannot be traced to a solvent party, including a fleet-wide attack, the Central Government should examine whether the Motor Vehicle Accident Fund contemplated by section 164B could be extended to it,⁷² since correlated loss is what sets cyber harm apart.⁷³ Section 110A should also be clarified, by rule or notification, so that a cybersecurity vulnerability reported to the Central Government counts as a defect for recall. None of this depends on India permitting driverless cars, since the draft rules apply to conventional vehicles with electronic control units.

⁷² Motor Vehicles Act 1988, s 164B (inserted by Act 32 of 2019).

⁷³ Channon and Marson (2021) 43 Computer Law & Security Review (arguing that mass hacking of vehicles on one software version requires a strategy for apportioning responsibility).

D. Conclusion and Observations

Cybersecurity liability in autonomous vehicles is a problem of allocation under uncertainty. A defect cannot be pointed to in the old way, an attacker stands between design and harm, and the evidence is held by the party most likely to be sued. The Union has answered by pairing a binding preventive regime with a strict-liability directive that names the problem, though neither has yet been tested in court. The United States has left the matter to tort and recall, has seen the litigation fail at the threshold, and is debating a bill that would add a plan but not a rule of liability. India has taken a preventive step in draft form and has a no-fault floor in section 164, but its consumer statute does not reach software, bystanders or third-party attacks.

The recommendations are modest by design. They borrow the Union's concepts and evidence rules, keep Indian institutions, and do not depend on a change of policy on driverless vehicles. Two caveats apply. The Indian rules are drafts and the European directive is not yet in application, so both may change. And the paper has dealt with civil liability, leaving aside the criminal responsibility of attackers and the terms of insurance contracts, which deserve separate study