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

Exploring Legal Liability in The Age of Autonomous Vehicles and Addressing Cyberattack Risks Under Indian Law

Ramachandra Subramanian

Student, B.A.LL.B.(Hons.) SASTRA Deemed University

ABSTRACT

Recent developments in technology have enabled the introduction of autonomous vehicles (AVs) into transportation systems. This has brought about the necessity to revise the existing laws in place owing to the significant challenges posed by AVs to the conventional concepts of determining legal liability in the event of an accident. This paper assesses whether and if so, to what extent these issues can be included and addressed within the boundaries of the existing legal framework with the forethought of technological advancements.

This paper sheds light upon the complexities faced while assigning liability in the event of an AV accident, which may involve various parties including manufacturers, software developers, vehicle owners, and operators by exploring various liability models ranging from product liability to operator negligence. The legal position in India is looked into while also considering the approaches of other legal systems across the globe.

Factoring in the emerging issue of cyberattacks on AVs, this paper also examines their potential impact on liability and the need for cybersecurity measures to mitigate risks. The adequacy of the law on this front is parallelly scrutinised. By identifying gaps in the Indian legal framework, this paper aims to contribute to the development of an adequate liability regime for the autonomous age and promote the safe and responsible development of AVs.

Keywords: Autonomous Vehicles, Accident Liability, Cybersecurity risks and Cyberattacks, Data Protection.

BACKGROUND OF THE STUDY

The advent of AVs represents a significant step forward in the evolution of the automobile industry by leveraging the potential of autonomous technology to expedite advancement. On one hand, equipped with advanced sensors, artificial intelligence, and sophisticated software, these vehicles have the potential to bring about a promising transformation in the transportation landscape by enhancing road safety, reducing traffic congestion, and optimizing fuel efficiency. On the other hand, such vehicles – rapidly moving closer toward widespread deployment by the day – also bring about legal challenges of complex natures, particularly with regard to accident liability. Vehicles that largely operate without any sort of human intervention push the bounds of traditional frameworks that assign liability on account of being built around the concept of human error. They are designed for human-driven vehicles and do not factor in the unique characteristics of AVs. Typically, the human driver is held accountable for accidents, but the

absence of such a driver in the case of AVs makes the task of determining liability very complicated and nuanced. The need for comprehension of the interplay between the various actors including manufacturers, software developers, vehicle owners, and operators involved in the development, maintenance, and operation of AVs, further obscures the question of liability.

In India, the legal regime governing motor vehicles is encapsulated in the Motor Vehicles Act, 1988. This legislation, formulated in a time period where the main focus was on driver negligence and human accountability, may not be equipped to adequately address the issues posed by AV accidents where the fault may lie with the software of the vehicle, or any actor such as the manufacturer or even unrelated third-party entities involved in data management and cybersecurity. The surge of AVs introduces yet another layer of complexity as a direct result of them being more technologically capable than conventional vehicles in the form of cyberattacks. Achieving such capability is only possible through the vehicles becoming increasingly connected and more reliant on sophisticated software systems. This inherent trait of AVs renders them vulnerable to hacking and other forms of cyber intrusion. If successfully carried out, a cyberattack on an AV could lead to catastrophic consequences in terms of physical harm, loss of property, and also fixing liability. On this front, the Information Technology Act, 2000, the legislation that governs cybersecurity and cybercrimes in India, is yet to fully engage with the challenges posed by AVs.

In addition to these legal frameworks, consumer protection laws, such as the Consumer Protection Act, 2019, and the Digital Personal Data Protection Act, 2023 (DPDPA), raise important questions regarding the rights of consumers in the event of harm or data breaches caused by AVs. The Consumer Protection Act provides avenues for redressal in cases of defective goods or services, potentially extending to AVs and their components, while the DPDPA ensures the protection of personal data collected and processed by such vehicles, adding another layer of responsibility for manufacturers and operators.

At the intersection of the realities of these emerging technologies and the existing legal framework in India is where this study finds its place. By exploring whether the current laws can be interpreted or adapted to address the unconventional risks associated with AVs – particularly in the context of cyberattacks – this paper aims to identify the gaps in the Indian legal system and provide suggestions for an adequate liability regime. Such a framework is crucial for handling the aftermath of accidents involving AVs. It will also play a vital role in fostering public trust in autonomous technology to facilitate its safe integration into society.

RESEARCH PROBLEM

As AVs become increasingly prevalent globally, the existing legal framework in India may not adequately address liability in the event of accidents, especially those resulting from cyberattacks. This paper explores whether these current laws can effectively determine liability in such cases, considering the unique challenges posed by AV technology.

LITERATURE REVIEW

1. **"Autonomous Vehicles and the Issue of Negligent Liability"** by Nandini Singh (*Indian Journal of Legal Review*)

   This paper focuses on the challenges of assigning legal responsibility in cases involving AVs. It highlights the complexity of determining who is accountable when the human driver is no longer in direct control of the vehicle. It identifies potential liable parties, such as the driver, the manufacturer,

and the software developer. While the driver has traditionally been held responsible under common traffic laws, the increasing role of technology means that liability may need to shift toward manufacturers or developers when AVs malfunction or make errors. The author explores existing global frameworks like the UK's Automated and Electric Vehicles Act of 2018, which establishes clear guidelines for liability when AVs are involved in accidents.

The paper falls short in exploring how Indian laws—such as the Motor Vehicles Act, 1988—handle these complexities. The act was formulated with human-driven vehicles in mind, and Ray does not address the limitations of this law in dealing with AVs. Additionally, the paper overlooks how liability might be distributed among different stakeholders in India, where regulatory standards are still evolving. It would benefit from a deeper analysis of how manufacturers, software developers, and even network providers could share liability in cases where software glitches or system failures cause accidents.

2. "**Cybersecurity and Autonomous Vehicles: Legal and Regulatory Challenges**" by Matthew Channon and James Marson (*Computer Law and Security Review: The International Journal of Technology Law and Practice*)

   This paper provides a comprehensive overview of the cybersecurity risks that AVs face and the legal frameworks in place to mitigate those risks, primarily focusing on the UK and global standards. It identifies key vulnerabilities in AV technology, such as hacking, spoofing, and data breaches, and explains how existing legal structures in advanced jurisdictions like the UK provide a model for mitigating these risks. The UK's Key Principles of Cyber Security for Autonomous Vehicles are highlighted as a best practice.

   The primary gap is the lack of focus on India's regulatory framework. While the paper explores how the UK and other advanced jurisdictions handle cybersecurity threats, it offers little insight into how Indian cybersecurity laws—particularly the Information Technology Act—address these issues. Furthermore, the article does not address the significant risks that come from the lack of specific cybersecurity protocols for AVs in India, nor does it propose any actionable steps for adapting global best practices to the Indian legal landscape.

3. "**Autonomous Vehicles and Product Liability: A Framework for Addressing Emerging Risks**" by Jack Boeglin (*Michigan Telecommunications and Technology Law Review*)

   This paper focuses on the evolution of product liability in the context of AVs. A liability framework that accounts for the complexities involved in accidents where technology replaces human decision-making is proposed. The paper suggests that manufacturers, software developers, and insurers could bear responsibility in cases of AV malfunctions. It emphasizes the difficulty of assigning fault when the AV system, rather than a human, is in control, and how traditional product liability laws must adapt to this new technology.

   While this paper provides a comprehensive view of product liability, it doesn't specifically address the cybersecurity vulnerabilities of AVs. The framework suggested does not consider liability in cases where cyberattacks compromise AV systems.

"**Cybersecurity and Autonomous Vehicles: Legal and Regulatory Challenges**" by Matthew Channon, Lucy McCormick, and Kyriaki Noussia (*Computer Law & Security Review: The International Journal of Technology Law and Practice*)

This paper emphasizes the cybersecurity risks inherent in AV systems and the need for robust legal and regulatory frameworks to address these issues. The paper analyzes the global cybersecurity standards

applied to AVs, such as encryption and secure data transmission, and highlights the significant vulnerabilities that AVs face from hacking, data breaches, and system hijacking. The authors call for clear cybersecurity protocols and legal reforms to ensure accountability in the event of cyberattacks on AVs.
While this paper extensively discusses cybersecurity risks and the need for stronger regulatory frameworks, it does not offer a structured liability model for incidents caused by cyberattacks.

4. "**Shifting Liability in the Age of Autonomous Driving: A Legal Perspective**" by Bryant Walker Smith (*Santa Clara Law Review*)

This paper examines the shift in liability as AV technology becomes more prevalent, focusing on the transition from human driver liability to the liability of manufacturers and service providers. It discusses the challenges in holding manufacturers accountable, especially in cases where AV systems malfunction or fail. The paper provides insights into how traditional negligence laws are likely to evolve in the face of increased automation, advocating for clearer distinctions between human and machine responsibility.
While this paper provides a valuable discussion on the shift in liability to manufacturers and service providers, it does not sufficiently explore the cybersecurity dimension, nor does it account for network providers and other parties involved in maintaining AV connectivity.

RESEARCH OBJECTIVE

The primary objective of this paper is to assess the effectiveness of the current Indian legal framework, specifically the Motor Vehicles Act, 1988, and the Information Technology Act, 2000, and related laws in addressing liability issues arising from accidents involving AVs, particularly those caused by cyberattacks. This study aims to identify gaps in the existing laws and propose recommendations for developing a comprehensive liability regime to adequately address the challenges posed by AV technology.

SCOPE AND LIMITATION OF STUDY

This study will primarily focus upon the Indian legal system concentrating on the relevant provisions, their interpretations, case laws and regulatory developments pertaining to the Motor Vehicles Act, 1988 and the Information Technology Act, 2000 and related laws to specifically examine the legal implications of accidents involving AVs caused by cyberattacks that target such vehicles in terms of liability. Insights as to how these issues are tackled in various other jurisdictions across the world have also been provided. The roles and responsibilities of key stakeholders such as manufacturers, software developers, vehicle owners, and operators are also looked into.
This study is confined to legal aspects and does not delve deeply into the technical intricacies of AV technology or cybersecurity measures thereby limiting the depth of analysis regarding technological solutions. Policy and regulatory frameworks addressing AVs are still evolving, which may restrict conclusions about the future legal landscape. And as AVs are relatively new and are yet to be integrated into the transportation network as far as India is concerned, the lack of availability of empirical data on accidents, cyberattacks and related cases is a constraint hindering effectiveness or applicability of conclusions. Moreover, given the rapid pace of technological advancements in the field of AVs and cybersecurity, the findings may be rendered outdated by emerging technologies and legal precedents.

RESEARCH METHODOLOGY

This paper employs a doctrinal legal research methodology, which focuses on a detailed analysis of existing laws, statutes, case laws, and legal frameworks to explore the adequacy of the current Indian legal system in addressing liability issues surrounding AVs and cyberattacks. The doctrinal approach is suitable for examining how established laws apply to emerging technologies like AVs and how legislative frameworks can be interpreted or reformed to accommodate these advancements.

The research draws on both primary and secondary legal sources:

- **Primary Sources**: Indian legislation, including the Motor Vehicles Act, 1988 and the Information Technology Act, 2000, are critically analyzed. Case laws, statutory provisions, and government reports related to AVs and cybersecurity form a key part of the primary data.
- **Secondary Sources**: The paper also reviews literature, academic papers, and legal commentaries on AV liability, particularly works on product liability, cybersecurity risks, and negligent liability. Comparative analyses of international frameworks including those such as the Automated and Electric Vehicles Act, 2018 (UK) and the German Road Traffic Act, are included to assess global best practices and their relevance to the Indian context.

In addition to examining Indian laws, the study incorporates a comparative analysis of regulatory frameworks from Germany, the UK, and the US (California). This comparative analysis is conducted to identify potential improvements in India's legal framework by learning from jurisdictions that have already addressed or begun addressing issues related to AV liability and cybersecurity.

CHAPTER 1 – INTRODUCTION

Pressing social and environmental issues such as traffic accidents, congestion, fuel usage, and emissions have catalysed the emergence of autonomous driving technology. AVs – which are automated or self-driving cars – assist human drivers in operating a motor vehicle or, in some cases, manage the vehicle entirely without the need for human involvement by employing sophisticated technology.[1] Depending on the level of automation in the vehicle, control actions such as acceleration, deceleration, lane changes, and parking can either be performed by a human driver or an automated system. This directly speaks to the AV's capability regarding the perception of its surrounding environment, including other vehicles, cyclists, traffic signals, pedestrians, and school zones.[2]

The Society of Automotive Engineers (SAE) — a global organization comprising engineers and technical experts from the aerospace, automotive, and commercial vehicle sectors — has established an industry benchmark for assessing the functionality of automated driving systems. This six-level classification plays an essential role in discussions related to the design, deployment, and regulation of autonomous vehicles, shaping relevant engineering, law, and public policy. It aims to clarify the capabilities and limitations of automated driving systems, facilitating better understanding and communication among consumers, engineers, and policymakers.

Ranging from Level 0, where the human driver is responsible for all driving functions, to Level 5, where vehicles operate fully autonomously in any setting without human input, each level marks a crucial stage

[1] J. M. Anderson, N. Kalra, K. D. Stanley, P. Sorensen, C. Samaras, and O. A. Oluwatola, Autonomous Vehicle Technology: A Guide for Policymakers, RAND Corporation, Santa Monica, CA, USA, 2016.

[2] F. M. Favar`o, N. Nader, S. O. Eurich, M. Tripp, and N. Varadaraju, "Examining accident reports involving au tonomous vehicles in California," PLoS One, vol. 12, 2017.

in the advancement of vehicle automation. The distinction between these automation levels is based on the involvement of the human driver and the automation system in performing the following driving tasks:

1. steering and throttle control,
2. monitoring the driving environment,
3. handling fallback responsibilities for the dynamic driving task (DDT), and
4. the system's capability to manage various autonomous driving modes.

Levels 0–2 rely on the human driver to perform part of or all of the DDT, and Levels 3–5 represent conditional, high, and full driving automation, respectively, meaning that the system can perform all the DDT while engaged.[3] This comprehensive definition of vehicle automation levels is widely applied in ongoing AV development efforts.

The six levels of driving automation, as specified by the SAE and broadly accepted by automotive manufacturers, regulators, and policymakers, are outlined below:

1. Level 0 (No Automation): All driving tasks are performed by the human driver. While vehicles may be equipped with basic warning systems like collision alerts, these do not constitute any form of automation.
2. Level 1 (Driver Assistance): Limited automation is introduced through the use of single automated systems that assist the driver, such as adaptive cruise control or lane-keeping assistance. The driver must remain actively engaged and is responsible for most driving tasks. While the human driver remains in control, the vehicle's automation system provides assistance during driving. These systems can enhance safety by providing support, but they do not enable full autonomy.
3. Level 2 (Partial Driving Automation): Multiple automated functions that allow for simultaneous control of steering and acceleration are combined, but the human driver must supervise the system, continue to monitor the environment, and be ready to take over control if necessary.
4. Level 3 (Conditional Driving Automation): The vehicle can manage all driving tasks in specific conditions but requires human intervention when the system encounters situations it cannot handle. This is designed for less complex scenarios such as highway driving. Although the driver is not expected to monitor the environment constantly, they must be ready to take over if the system requests it.
5. Level 4 (High Driving Automation): Vehicles are capable of fully autonomous driving within designated operational domains. Complete autonomy in controlled environments such as urban settings is possible. Human control may be required in in adverse conditions or situations outside the vehicle's programming.
6. Level 5 (Full Driving Automation): No human input is necessary for driving in any environment.
7. Vehicles at this level are equipped to fully operate autonomously under all conditions, eliminating the need for a driver, though the option for manual control remains.[4]

Human drivers and vehicle systems can engage in the driving process to varying extents, as illustrated by the levels of automation. This indicates that safety concerns differ significantly between partially, highly,

[3] Wang, Jun, Zhang, Li, Huang, Yanjun, Zhao, Jian, Safety of Autonomous Vehicles, *Journal of Advanced Transportation*, 2020, 8867757, 13 pages, 2020. https://doi.org/10.1155/2020/8867757

[4] F. M. Favar`o, N. Nader, S. O. Eurich, M. Tripp, and N. Varadaraju, "Examining accident reports involving autonomous vehicles in California," PLoS One, vol. 12, 2017. ; SAE International, Surface Vehicle Recommended Practice (R) Taxonomy and Definitions for Terms Related to Driving Automation Systems for On-Road Motor Vehicles, SAE International, Pittsburgh, PA, USA, 2018. ; United States Department of Transportation, Automated Vehicles for Safety, United States Department of Transportation, Washington, DC, USA, 2019, Automated Vehicle Safety | NHTSA.

and fully autonomous vehicles. In modes of no automation, partial automation, or high automation, the interaction between human drivers and machine systems poses a considerable challenge to the safety of AVs. Conversely, in fully autonomous modes, the reliability of both software and hardware becomes a critical factor. In essence, as vehicles incorporate more advanced autonomous technologies, the system's complexity increases, raising concerns about stability, reliability, and overall safety.[5]

CHAPTER 2 – EXISTING LEGAL FRAMEWORKS REGARDING AUTONOMOUS VEHICLES IN INDIA

1. The Motor Vehicles Act, 1988

The Motor Vehicles Act, 1988 (MV Act) does not contain any specific provisions that address AVs nor does it permit their use or testing on Indian roads. Section 109(1) of the Act[6] mandates every motor vehicle to be designed in such a way that ensures that the person driving the vehicle has effective control over it at all times. This severely limits the extent of AVs in India, indicating that AVs of Level 4 and above would not be covered under the MV Act, implying that such AVs are illegal and not allowed in India. But it cannot be denied that AVs leverage groundbreaking innovation to revolutionise the transportation sector. Automobiles fitted with an advanced combination of sensors and cameras, equipped with artificial intelligence promise to increase the safety, effectiveness, and convenience of transportation by being able to navigate roads and function independently without the need for any human intervention. They are capable of detecting and responding to their environment, accounting for other vehicles, pedestrians, and even traffic signs and signals on their own without human input. This has in turn incentivised global efforts to develop appropriate regulatory frameworks to ensure the responsible deployment and use of AVs. And although AVs are a reality in some countries across the globe, they are still very much in their infancy in India.

The issue of the legality of AVs in India has to be viewed through the lens of Section 2B, inserted through the Motor Vehicles (Amendment) Act of 2019 with the object of promoting innovation. The Central Government may – subject to such conditions prescribed by it – exempt certain types of mechanically propelled vehicles from the application of the provisions of the MV Act in order to promote innovation, research, and development in the fields of vehicular engineering, mechanically propelled vehicles and transportation in general. A liberal interpretation of this provision opens up the possibility of AVs being exempted from the provisions of the MV Act, thereby permitting their research, development, and testing within the territory of India.

Uber founder and former CEO Travis Kalanick, once remarked in late 2016 that India would be the last place in the world to get self-driving cars after experiencing the unpredictable traffic and chaotic driving pattern of Delhi roads.[7] Despite there being only a handful of demonstrations and prototypes currently in operation, Tata Motors, Mahindra & Mahindra, and the Indian Institute of Technology (IIT) Madras are among the Indian corporations working on self-driving automobile technology. It is important to keep in mind that this field is not exclusive to such established players only. In June 2023, India's first fully autonomous vehicle, the zPod was launched by Minus Zero, India's first startup with a mission to build fully autonomous vehicles in India.[8] In March 2024, Swaayatt Robots – another startup – successfully

[5] Supra 3
[6] The Motor Vehicles Act, 1988, §109, No. 59, Acts of Parliament, 1988 (India).
[7] Uber CEO Travis Kalanick says India will be the last place to get autonomous cars – Firstpost
[8] India's first autonomous car zPod is truly a game changer (indiaai.gov.in)

conducted a demonstration showcasing their substantial progress in developing Level 5 AVs.[9] Therefore, it is evident that there is a growing presence of stakeholders in India focusing on AV technology, setting up a future where competition and innovation among various players will drive the advancement and adoption of AVs at a faster pace.

2. The Consumer Protection Act, 2019

The Consumer Protection Act, 2019 (CP Act) comes into play for safeguarding consumer rights in India, expanding to the context of evolving technologies such as AVs. The CP Act brings in provisions detailing product liability, making the product manufacturer, service providers, and product sellers accountable for any harm resulting from their defective products or services. Issues in the design, production, or maintenance of their vehicles may expose manufacturers to liability in instances where such fault is the primary cause of an injury. Manufacturers are required to be diligent and take reasonable care in the design, production, and testing of their vehicles. This aspect is particularly relevant for autonomous vehicles, where the technology's complexity raises significant liability questions. Should an autonomous vehicle be faulty or malfunction, the law ensures that consumers can seek compensation from manufacturers or sellers under product liability actions, as defined in Sections 2(34) and 2(35) of the Act[10] to align with consumer expectations in the face of potential risks associated with autonomous driving technologies.

Innovations in AVs can no longer be said to lie within the sole domain of traditional car manufacturers and their component suppliers due to the rising demand for automation, safety electronics, mobile connectivity, and entertainment systems. Advancements in information technology have opened up the automotive market to new unconventional entrants who are driving much of the progress such as tech companies, software developers, and startups specialising in sensory and mapping technology. This has pushed established players to either adapt or risk losing market share. Consequentially, Original Equipment Manufacturers (OEMs) may increasingly shift away from their vertically integrated, asset-heavy business model to satisfy demand. This suggests that as manufacturers gain more control and information about their products and users, their obligations regarding safety and accountability will expand considerably.[11]

The CP Act also deals with issues regarding misleading representations[12] and breach of warranty[13] among others. The right to consumer education has also been included to ensure that consumers are aware of the operations of AVs and can take control during emergencies.

3. The Information Technology Act, 2000

AVs can be described as vehicles that are computer-controlled which use various sources of data to evaluate their surroundings and manage driving functions.[14] They draw upon a combination of rotating lasers to map the environment in fine detail – producing up to just shy of one million data points per second – along with a network of sonar, radar, and cameras, all of which provide supplementary data to help the vehicle maintain an awareness of its surroundings. Cellular or wireless connectivity allows them to receive real-time updates about road conditions and congestion and as such, autonomously redirect

[9] IITian develops self-driven cars in Bhopal, runs in traffic on autonomous technology - The Economic Times Video | ET Now (indiatimes.com)
[10] The Consumer Protection Act, 2019, §2(34) and 2(35), No. 35, Acts of Parliament, 2019 (India).
[11] Autonomous vehicles: The legal landscape in the US | United States | Publications | Knowledge | Global law firm | Norton Rose Fulbright
[12] The Consumer Protection Act, 2019, §89, No. 35, Acts of Parliament, 2019 (India).
[13] The Consumer Protection Act, 2019, §84(1) No. 35, Acts of Parliament, 2019 (India).
[14] D Glancy, 'Privacy in Autonomous Vehicles' (2012) 52 Santa Clara L. Rev. 1171, 1174.

themselves around traffic.[15] And when a vehicle collects such data and links it to a specific identifiable individual, the data becomes personal in nature.[16] The integration of AV technology often necessitates the gathering of vast amounts of personal data, which can lead to concerns about misuse and unauthorized access to sensitive information. As this data qualifies as sensitive, the safeguarding of such data becomes very crucial. Any misuse or tampering could lead to a breach of privacy and infringe upon an individual's fundamental rights.

Sections 2(i)[17], (j)[18], and (k)[19] of the Information Technology Act, 2000 (IT Act) provide foundational definitions relevant to computer systems, which can be directly applied to the ecosystem of AVs. These provisions help situate AVs within India's legal framework for cybersecurity and data protection.

Section 2(i) defines "computer" as an electronic or other high-speed data processing device capable of performing logical, arithmetic, or memory functions. AVs rely heavily on advanced onboard computer systems to execute tasks such as navigation, obstacle detection, and decision-making. These systems integrate multiple components, such as sensors, cameras, and processors, to analyse real-time data and make autonomous decisions. For example, the central processing unit of an AV processes information from LiDAR and radar systems to detect and respond to obstacles, enhancing safety and operational efficiency. In the legal context, any hacking, tampering, or unauthorized access to these onboard systems can be prosecuted under the IT Act.

Section 2(j) refers to a "computer network" as the interconnection of computers through communication links. AVs operate within a sophisticated network ecosystem, encompassing Vehicle-to-Vehicle (V2V) and Vehicle-to-Infrastructure (V2I) communications. These networks enable AVs to share data on traffic, weather, and road conditions, supporting their autonomous functions. However, these interconnections also expose AVs to cybersecurity risks, such as hacking or denial-of-service attacks. The IT Act addresses such vulnerabilities, holding offenders accountable under provisions like Section 66, which penalizes unauthorized access or cyberattacks.

Section 2(k) broadens the scope to "computer resource," encompassing computers, communication devices, and interconnected systems. This expansive definition captures the entirety of the AV ecosystem, including its hardware, software, and communication frameworks. AVs collect and process extensive data through their interconnected components, qualifying them as "computer resources."

Together, these sections establish a basis for addressing the cybersecurity and operational challenges posed by AVs. The IT Act also subjects the entities that collect and store personal data to certain obligations and liabilities to ensure that the privacy rights of individuals are duly protected. The IT Act governs the handling of personal data, including that collected by AVs. It lays down strict regulations regarding the processing, storage, and protection of sensitive personal data or information (SPDI), which includes location and biometric data, which are relevant in the context of AVs.

Accordingly, AV manufacturers and service providers are treated as intermediaries[20] under the IT Act, depending on the extent to which they collect and process personal data. They are imposed with a duty to implement reasonable security measures to safeguard the data they process. Adoption of practices such as encryption, anonymization, and using secure servers to protect the integrity of the data collected by AVs

[15] T Lee, 'Self-Driving Cars are a Privacy Nightmare. And it's Totally Worth it' *Washington Post* (Washington 21 May 2013)
[16] Supra 9, 1175
[17] Information Technology Act, No. 21 of 2000, § 2(i), Acts of Parliament, 2000 (India).
[18] Information Technology Act, No. 21 of 2000, § 2(j), Acts of Parliament, 2000 (India).
[19] Information Technology Act, No. 21 of 2000, § 2(k), Acts of Parliament, 2000 (India).
[20] Information Technology Act, No. 21 of 2000, § 2(w), Acts of Parliament, 2000 (India).

is mandated by the IT Act.[21] Any company or person who causes wrongful loss or gain to an individual due to data breach or unauthorized access as a result of negligence in implementing and maintaining reasonable security practices is liable to compensate the affected party.[22] The unlawful disclosure of personal information is also covered by the Act. Penalties are imposed for the disclosure of personal information without obtaining consent that results in wrongful loss or gain to the data subject on individuals or entities, including AV companies.[23] This provision is significant for AV technology, where sensitive personal data is frequently shared with various entities, such as cloud service providers, mapping services, or analytics platforms. Compliance with this section is critical to prevent unauthorized sharing and ensure data protection in the AV ecosystem.

Since AVs are heavily reliant on computer systems and internet connectivity to function, they become particularly vulnerable to cyberattacks, data manipulation, or system hijacking. Computer-related offenses such as hacking, unauthorized access, and identity theft are addressed by the IT Act which makes any person who accesses a computer system without permission and extracts data or causes damage to the system, subject to punishment including imprisonment and fines.[24]

4. Digital Personal Data Protection Act, 2023

In light of the Digital Personal Data Protection Act, 2023 (DPDP Act), developers and manufacturers of AVs are required to align their data collection practices with this legal framework. Not all data collected by autonomous and connected vehicles is essential for their technical operation. For instance, data entered by the driver or user for infotainment purposes or personalized comfort settings is often not required for driving functionality. While it is not disputed that these features enhance the user experience, the collection of such data may not be technically necessary for the vehicle to function autonomously, raising privacy concerns. The DPDP Act makes it necessary to adhere to principles such as data minimization, purpose limitation, transparency, and accountability to limit the scope of data collection to what is necessary for specific operational purposes and ensure secure data storage and processing. The data so collected must not be stored longer than required. It emphasizes transparency in data processing activities, requiring companies to disclose what data is collected, how it is used, and for how long it will be retained.

The DPDP Act follows a user-centric approach to data collection. Users must be informed clearly about the types of data collected and the purposes for which the data is processed. This highlights the importance of informed consent, wherein AV users should be made aware of how their data is being collected, used, and shared with third parties, if applicable. The law also provides individuals with rights such as the right to access their data, the right to correction, and the right to erasure, which will enable AV users to have more control over their personal data.

The Act also underscores the importance of the lawful processing of data. This means that developers and manufacturers of AVs must ensure that personal data is collected and processed only when there is a legitimate, lawful basis for doing so. Processing personal data is considered lawful only if it is necessary for the performance of a contract, compliance with legal obligations, or for legitimate interests pursued by the data controller, provided these do not override the fundamental rights and freedoms of the data subject.[25] In the context of AVs, this implies that data collection for purposes not essential to the vehicle's

[21] Rule 4(2), Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021
[22] Information Technology Act, No. 21 of 2000, § 43A, Acts of Parliament, 2000 (India).
[23] Information Technology Act, No. 21 of 2000, § 72A, Acts of Parliament, 2000 (India).
[24] Information Technology Act, No. 21 of 2000, § 66, Acts of Parliament, 2000 (India).
[25] Digital Personal Data Protection Act, No. 22 of 2023, § 4, Acts of Parliament, 2023 (India)

core functioning—such as personalized infotainment features—must be justified through explicit user consent. If an AV collects data for non-essential services, users must have the ability to withdraw consent easily, and upon doing so, the associated data should no longer be processed or retained.

CHAPTER 3 – APPROACHES TO AV LIABILITY

Concerning liability in case of accidents, Section 2(34)[26] of the CP Act, dealing with product liability makes the product manufacturer or product seller as the case may be, responsible for any harm caused by the defective product. On the contrary, Section 140[27] of the MV Act provides that the claimant may seek compensation from the owner of the vehicle if disablement has been caused due to a motor vehicle accident even if it was caused without any default or neglect on the part of the owners. This ambiguous predicament highlights the absence of a clearly defined mechanism for the claimant or victim to assert their remedy. This leads to complications when dealing with liability for accidents caused by AVs due to the absence of laws determining the onus of liability in such instances.

The trolley problem presents a scenario where a trolley operator loses control, leading the trolley toward a path that would result in the deaths of five innocent individuals. However, the operator has the option to divert the trolley onto another track, which would cause the death of only one person.[28] In a slight variation of the scenario, it is a bystander, rather than the driver, who has the ability to redirect the trolley.[29] To assign liability for such an accident, let's assume that in our analysis, the driver represents either the vehicle's driver or occupants, and the bystander symbolizes the autonomous vehicle (AV), encompassing its owners, manufacturers, AI developers, or insurers.

The key distinction here is that while the bystander is physically present during the incident, in some cases, the bystander would have acted in advance—the owner would have purchased the AV knowing all the potential risks, the manufacturer would have ensured the AV's production and sale met all necessary standards, the AI programmers would have preemptively designed the system to handle such scenarios, and the insurer would have agreed to cover damages and related costs.[30] Now, let's consider different scenarios involving both partially autonomous vehicles (PAVs) and fully autonomous vehicles (FAVs) to determine how liability should be assigned.

In PAV Scenario I, the driver or occupants are able to regain control of the vehicle either after receiving a warning from the AV or by noticing that the AV has malfunctioned.

In PAV Scenario II, the driver or occupants are unable to regain control because they are either unable to disable autopilot, fail to receive a warning from the AV, or fail to notice that the vehicle is no longer under control.

In FAV Scenario I, the driver or occupants have no option to take back control and are entirely reliant on the AV system.

In PAV Scenario I, it's clear that responsibility falls on the driver or occupant, as they had the opportunity to regain control. However, in PAV Scenario II and FAV Scenario I, where control shifts from the driver or occupant to the AV, doesn't it make sense to transfer liability from the individual to the AV? Or should

[26] The Consumer Protection Act, 2019, §2(34), No. 35, Acts of Parliament, 2019 (India).
[27] The Motor Vehicles Act, 1988, §140, No. 59, Acts of Parliament, 1988 (India).
[28] F M Kamm, 'The Use and Abuse of the Trolley Problem' in S Matthew Liao (ed) Ethics of Artificial Intelligence (Oxford University Press 2020)
[29] *Ibid*
[30] *Ibid*

we still hold the driver accountable, either because they attempted to regain control unsuccessfully or simply because they were present in a vehicle over which they had no control?

To address these questions, it's essential to explore the notions of liability. These legal frameworks will help determine whether liability should remain with the driver or shift to the manufacturers, programmers, or others involved in the AV's operation.[31]

Driver Liability

With the introduction of autonomous vehicles (AVs) in India, there will be an inevitable need to shift liability from the driver to the manufacturer or service provider when product defects are involved.[32] Traditionally, liability for accidents caused by motor vehicles has been attributed to the driver. For instance, in the case of Kaushnuma Begum[33], the court attributed technical malfunction back to the driver, applying the principle of strict liability. However, with AVs, the software controls many aspects of the vehicle, necessitating a legal distinction between faults arising from the manufacturer and those attributable to the user.

Globally, the trend is moving toward holding manufacturers accountable for AV-related accidents. In line with this, the Law Commission of England and Wales, along with the Scottish Law Commission, has proposed recommendations that would shift liability away from drivers and onto manufacturers in cases of technical defects. These include both preventive and post-incident measures to ensure safe use of AVs, as well as a two-stage legal process for approval and authorization to ensure compliance. In the U.S., the Federal Motor Vehicle Safety Standards also set expectations for manufacturers regarding safety standards in vehicles.

In India, strict liability has often been applied to drivers, as evidenced by the reliance on the precedent set in Rylands v Fletcher[34], which was used in Kaushnuma Begum[35] to impose liability on the driver when a vehicle's wheel burst. Some legal interpretations suggest that this absolute liability of drivers could extend to autonomous vehicles as well. Under this approach, accidents caused by AVs could still be attributed to the driver, with limited defenses available, such as proving fault on the part of the plaintiff or an act of God.

However, with the implementation of product liability laws in India, accidents resulting from product defects should, in principle, transfer liability to the responsible party—likely the manufacturer or another entity involved in the vehicle's design or operation.[36] The challenge, though, lies in pinpointing the exact cause of an accident in AVs, making it more complex to determine fault.

In common law, users of ships or planes can be held responsible for negligent use of an autopilot system. Similar to traditional vehicle accidents, human error is often the primary cause of such incidents. However, in cases involving automated technology, the operator may not be at fault if a system malfunction occurs while the vehicle is in fully autonomous mode, as they are not directly responsible for the accident or resulting harm.

[31] Mythili Srinivasamurthy, Autonomous Vehicles and Complexities in Allocation of Liability, 1 JUS CORPUS L.J. 360 (June-August 2021).

[32] Thomas Kadner Graziano, 'Cross-Border Traffic Accidents in the EU-the Potential Impact of Driverless Cars' (2016) European Parliament, Directorate-General for Internal Policies, Policy Department C: Citizens' Rights and Constitutional Affairs, PE 571.362, 37

[33] Kaushnuma Begum and Ors v The New India Assurance Co. Ltd., AIR 2001 SC 485.

[34] Rylands v Fletcher, (1868) LR 3 HL 330.

[35] Supra 33

[36] CPA § 39(1) (e).

That said, manufacturers often shift liability to operators, arguing that they bear some level of fault in various degrees, which complicates the issue. This shifting of blame highlights an area that will need careful consideration by future lawmakers. Courts will need to assess operator negligence on a case-by-case basis to determine the appropriate allocation of liability.

Owner Liability

For conventional vehicles, international regulations have long imposed responsibilities on both the manufacturer and the driver, dating back to the International Convention on Motor Traffic, established in Paris in October 1909. More recently, the United Nations Economic Commission for Europe (UNECE) has developed conventions requiring countries to adopt consistent standards on issues like road signage. The most relevant is the 1968 Vienna Convention (as amended)[37], which contains notable provisions under Article 8:

1. Every moving vehicle or combination of vehicles must have a driver.
2. [Not applicable—concerns animals]
3. Every driver must have the physical and mental capability to drive and be in a fit condition to do so.
4. Drivers of power-driven vehicles must possess the necessary knowledge and skill for driving, though this does not prevent learner drivers from practicing under domestic law.
5. Drivers must always be able to control their vehicle.

Annex 5 of the convention outlines Technical Conditions for motor vehicles and trailers, listing requirements like braking and lighting. The convention assumes vehicles meet these standards, with the driver being responsible for safety during operation. For AVs of Levels 3 and below, these vehicles comply with Article 8 because they still involve human drivers. However, for Levels 4 and 5 AVs, which lack a human driver, a question arises about who bears the responsibilities traditionally held by the driver.

Currently, prototype testing of AVs is conducted by major automotive or technology companies that develop AV systems. These companies assume both the responsibilities of the vehicle's manufacturer and those of the driver, making the distinction between the two roles irrelevant at this stage. The situation becomes more complex when AVs are leased or sold to companies like delivery services or taxi firms, or even to private individuals. In such cases, the purchasers or their employees become the vehicle's operators, but they cannot be considered drivers, nor do they have the expertise of manufacturers to ensure the safety of the automated systems.

Section 140 of the MV Act outlines the principle of No Fault Liability in cases of motor vehicle accidents that result in death or permanent disablement. According to this provision:

- The owner or insurer of the motor vehicle involved in an accident is liable to pay compensation to the victim or their legal heirs, irrespective of whether the accident occurred due to negligence.
- The claimant does not need to prove fault or negligence on the part of the driver, owner, or any other party.
- Compensation is payable for death or permanent disablement without requiring the victim to establish fault, ensuring that victims receive timely financial support.

  Section 163A of the Act further strengthens the principle of No Fault Liability by providing for a structured compensation scheme. This provision establishes:
- Compensation to be paid in cases of death or permanent disablement caused by a motor vehicle accident, regardless of fault or negligence.

[37] United Nations Economic Commission for Europe (UNECE), Convention on Road Traffic, Vienna, November 1968.

- The victim or their legal heirs are entitled to compensation based on a predetermined formula, without needing to prove that the accident was caused by the fault of the driver or owner of the vehicle.

It also underscores that to benefit from No Fault Liability, the claimant does not have to prove that the driver or owner was at fault. This provision is based on the idea of social welfare and is intended to ensure justice for accident victims. In cases where negligence or fault cannot be clearly established, this principle provides an avenue for compensation, promoting the welfare state principle embedded in India's legal framework.

Many argue that the principle of No Fault Liability offers an efficient way to handle AV accidents, as it reduces the need for protracted litigation over technical faults and system failures, placing the immediate burden of compensation on vehicle owners or their insurers.[38]

Looking forward, ownership models for AVs will play a critical role. Without a driver, the obligation to ensure safe operation must lie with a competent operator, capable of handling this responsibility. This may limit the capacity of certain companies or individuals to own or lease AVs, as they would need to demonstrate the ability to manage the vehicle's automated systems safely.[39]

Tort Liability

(i) Negligence

Traditional negligence doesn't serve as an adequate theory of liability when an AV causes an accident. Under common law, a vehicle owner who allows someone else to drive isn't held liable for the driver's negligence.[40] One state supreme court has also ruled that a driver's negligence cannot be automatically attributed to the owner or principal simply because they were present in the vehicle at the time of the incident.[41] In the case of self-driving AVs, the owner, acting as a passenger, isn't considered to be operating the vehicle.[42] As such, if a dangerous situation arises, the passenger may be unable to intervene and therefore cannot be expected to exercise reasonable care to prevent harm to others.

Given this, courts are unlikely to impose liability on a passenger who lacks the ability to intervene. Since the automated system is essentially regarded as the "driver" in an AV, the owner—even as a passenger—should not be held liable under negligence. Instead, accidents caused by the automated system may raise product liability concerns against the manufacturer rather than involving negligence claims.

(ii) Strict Liability

Strict liability is similarly not an appropriate theory of liability for crashes involving self-driving AVs. Strict liability applies to "abnormally dangerous activities," which courts have long ruled does not include driving vehicles, as this is considered common usage rather than an inherently dangerous activity. Activities such as explosive blasting, storing radioactive or hazardous materials, and keeping wild animals are examples of abnormally dangerous activities, but automobiles do not fall into this category.

In 1907, a US appellate court noted that it was not the inherent danger of automobiles that was feared, but rather the reckless behavior of those driving them. Strict liability has been argued as potentially relevant for early AV users, with some plaintiffs claiming that such users take a risk by using the technology and should be held responsible under strict liability principles, as AV operation could be viewed as an

[38] Anderson, J., Kalra, N., Stanley, K., Sorensen, P., Samaras, C., & Oluwatola, O. (2014). Autonomous Vehicle Technology: A Guide for Policymakers. RAND Corporation.

[39] Roger Kemp, Autonomous Vehicles - Who Will Be Liable for Accidents, 15 DIGITAL EVIDENCE & ELEC. SIGNATURE L. REV. 33 (2018).

[40] Morris v. Snappy Car Rental, Inc., 637 N.E.2d 253, 254 (N.Y. 1994).

[41] Reeves v. Harmon, 475 P.2d 400, 403 (Okla. 1970).

[42] Young v. Masci, 289 U.S. 253, 255-56 (1933).

ultrahazardous activity.[43] These plaintiffs may argue that individuals engaging in ultrahazardous activities are more aware of the associated risks and should bear the costs, regardless of fault.

However, tort law tends to accommodate technological advances by refusing to impose strict liability on distributors of new or innovative technologies.[44] Thus, since self-driving vehicles are not deemed ultrahazardous, and because tort law allows for technological progress, vehicle owners should not be held liable under strict liability. As AVs evolve, owners will have less control over risks, leading to a decrease in owner liability and an increase in manufacturer liability, as the latter will bear greater responsibility for managing those risks.

Product Liability

The CP Act defines "product liability" as the responsibility of the product manufacturer, product seller, or service provider to compensate for any harm caused to a consumer by a defective product or a deficiency in service[45]. The term "harm" under the Act includes physical injury, mental agony, property damage, or even death[46].

A product is considered "defective" if it has any fault, imperfection, or shortcoming in quality, quantity, potency, purity, or standard that a person is reasonably entitled to expect[47]. In the context of AVs, this includes defects in the software systems, sensors, hardware, or other components essential to the vehicle's autonomous functions.

The Act stipulates three main categories of liability:

1. Liability of the manufacturer: Liability for defects in design, manufacture, or a failure to provide adequate warnings or instructions. A manufacturer is liable for any harm caused by a product defect, irrespective of whether the consumer establishes negligence or intent.[48]
2. Liability of the seller: A seller can also be held accountable if they sell a product that is defective or does not conform to express warranties.[49]
3. Liability of the service provider: Service providers can be held liable for any deficiency in the services provided in connection with the product such as inadequate maintenance or faulty software updates.[50]

In the case of AVs, these provisions can be applied to both the manufacturers of the autonomous driving systems and the entities responsible for selling or servicing the vehicles.

- **Application of Product Liability to Autonomous Vehicles**

(i) Manufacturer Liability

The manufacturer of an autonomous vehicle, whether a domestic company or a foreign corporation supplying AVs in India, can be held liable for harm caused by defects in the vehicle's design, software, or hardware. Autonomous vehicles rely on complex algorithms, sensors, cameras, and other hardware components to navigate and make decisions without human input. A defect in any of these components can lead to accidents or malfunctions, which may cause harm to passengers, other road users, or property. Under the CPA, 2019, a manufacturer is strictly liable for defects in the product, meaning the consumer does not need to prove negligence or fault. This principle of strict liability is critical in the context of AVs,

[43] Lewis v. Amorous, 59 S.E. 338, 340 (Ga. Ct. App. 1907).
[44] James A. Henderson, Jr., Tort vs. Technology: Accommodating Disruptive Innovation, 47 ARIZ. ST. L.J. 1145, 1159 (2015).
[45] Supra 26
[46] The Consumer Protection Act, 2019, §2(22), No. 35, Acts of Parliament, 2019 (India).
[47] The Consumer Protection Act, 2019, §2(10), No. 35, Acts of Parliament, 2019 (India).
[48] The Consumer Protection Act, 2019, §2(36), No. 35, Acts of Parliament, 2019 (India).
[49] The Consumer Protection Act, 2019, §2(37), No. 35, Acts of Parliament, 2019 (India).
[50] The Consumer Protection Act, 2019, §2(42), No. 35, Acts of Parliament, 2019 (India).

as it places the burden on manufacturers to ensure the safety of their products before they are released into the market.

For example, if an autonomous vehicle's sensor system fails to detect an obstacle on the road, leading to an accident, the manufacturer could be held liable for any injuries or property damage caused by the malfunction. The consumer would not need to demonstrate that the manufacturer was negligent in designing the system, as long as it can be established that the product was defective.

In *Toyota Motor Corp. Unintended Acceleration Litigation* (2013), Toyota faced claims for defects in the software that allegedly caused unintended acceleration. Although not related to cyberattacks, the case emphasizes manufacturers' responsibility for software in vehicles, which can be a reference point for future AV-related cases.

(ii) Seller Liability

Sellers of AVs may also be liable under the CPA, 2019, if they sell a defective product or one that does not conform to the warranties provided. Sellers must ensure that the products they distribute are safe and meet the advertised standards. If a defect in the AV arises from a failure by the seller to adhere to these obligations, the seller can be held responsible for any harm caused.

An important point of consideration is the role of third-party sellers and online marketplaces in the sale of autonomous vehicles. Under the CPA, 2019, online platforms are subject to similar product liability rules as traditional sellers if they are directly involved in the sale of the product. This provision is relevant as AVs may increasingly be marketed and sold through online platforms.

(iii) Service Provider Liability

Autonomous vehicles, like other high-tech products, require regular maintenance and software updates. The service providers responsible for these activities can also be held liable for any deficiencies that cause harm. For instance, if a service provider fails to install a crucial software update that enhances the vehicle's obstacle detection system, and this leads to an accident, the service provider could be held liable under the CPA, 2019.

Additionally, service providers are responsible for ensuring that any parts replaced or software updates installed meet the required standards of safety and functionality. A failure to do so could result in liability for harm caused to consumers.

In *Anderson v. Vanden Dorpel*[51], the court acknowledged that service providers, including developers, must exercise reasonable care in their services. A similar principle can be applied to AV software developers, particularly if a failure to meet industry standards for cybersecurity leads to harm.

CHAPTER 4 – CYBERATTACKS IN AVS

Cyberattacks on AVs pose significant threats due to their reliance on digital networks and internet connectivity. As these vehicles become increasingly integrated into urban environments, they are susceptible to various cyber threats such as data breaches, spoofing, denial-of-service attacks, and ransomware. The consequences of such cyberattacks can range from financial losses and data compromises to severe safety hazards, including the potential for loss of life. Understanding the implications of these cyber vulnerabilities is essential for manufacturers, software developers, and operators to ensure the safe deployment of AV technology.

[51] Anderson v. Vanden Dorpel, 673 N.E.2d 129, 129 (Ill. 1996)

Computers play a crucial role in enhancing vehicle stability, safety features, electronic fuel management, and theft prevention systems. Modern vehicles also integrate functionalities similar to smartphones, such as voice commands, mobile data, web browsing, gaming, and other entertainment options. However, these advancements, aimed at making vehicles more connected and autonomous, introduce significant security risks. These technologies expose vehicles to potential cyberattacks, making them vulnerable to threats. Numerous researchers have demonstrated the potential attack surfaces, highlighted the vulnerabilities, and shown how remotely connected vehicles and infrastructure could lead to life-threatening situations.[52]

On this front, there are three main methods that hackers could exploit to gain control over AVs. They are:

1. Exploiting Software Vulnerabilities: Hackers can exploit weaknesses in various electronic components of an AV to gain unauthorized access. Past studies have demonstrated attacks on infotainment systems[53], Bluetooth connections[54], and cellular networks[55]. These vulnerabilities make it possible for attackers to take control of critical vehicle functions remotely.
2. Physical Hacking via Malicious Devices: Physically plugging a device, such as a laptop, into the onboard diagnostics (OBD-II) port gives hackers access to the vehicle's internal Controller Area Network (CAN). Once inside the CAN, attackers can launch various cyberattacks, allowing them to compromise vital systems and potentially take control of the vehicle.[56]
3. Hacking the AV Ecosystem: The AV ecosystem includes vehicle-to-infrastructure (V2I) and vehicle-to-vehicle (V2V) communications, which are vulnerable to cyberattacks. These communications, typically enabled by protocols like Dedicated Short-Range Communication (DSRC) or 5G, are vulnerable to attacks such as denial of service (DoS), GPS spoofing[57], and location tracking[58]. Further, over-the-air software updates, necessary for AV maintenance, have been identified as a critical vulnerability[59], potentially allowing widespread exploitation of multiple AVs if compromised. Additionally, charging stations and diagnostics centers may become attack points for hackers to gain access to AVs.

Supply chain attacks or the discovery of zero-day vulnerabilities (previously unknown software flaws) present another risk, as they allow hackers to target AVs before manufacturers have time to develop countermeasures.

Based on various studies, four broad categories of plausible hacks on AVs have been identified. Each type of hack presents unique risks, ranging from system disruption to data theft, and can have varying degrees of impact depending on the circumstances. They are:

Disabling Attacks

[52] Checkoway S, McCoy D, Kantor B, Anderson D, Shacham H, Savage S et al. Comprehensive experimental analyses of automotive attack surfaces. In Proceedings of the 20th USENIX Security Symposium. USENIX Association. 2011. p. 77-92. (Proceedings of the 20th USENIX Security Symposium).

[53] Miller, C., & Valasek, C. (2014). A Survey of Remote Automotive Attack Surfaces. *IOActive Report*.

[54] Dunning, J. (2010). Taming the Blue Beast: A Survey of Bluetooth Based Threats. *IEEE Security & Privacy, 8*(2), 20-27.

[55] Wright, R. (2011). Cellular Network Threats: Hacking Techniques and Tools. *Journal of Cyber Security*, 3(1), 45-54.

[56] Koscher, K., Czeskis, A., Roesner, F., Patel, S., Kohno, T., Checkoway, S., ... & Savage, S. (2010). Experimental Security Analysis of a Modern Automobile. *Proceedings of the IEEE Symposium on Security and Privacy,* 447-462.

[57] Sumra, I. A., Hasbullah, H., & Al-Hubaishi, M. (2011). Trust and Trusted Computing in VANET. *Proceedings of the International Conference on Information Technology*, 197-203.

[58] Laurendeau, C., & Barbeau, M. (2006). Threats to Security in DSRC/WAVE. *Proceedings of the 5th International Conference on Ad-Hoc Networks & Wireless,* 266-279.

[59] Sampath, S., Lu, Y., & Mo, J. (2007). Securing Over-the-Air Firmware Updates for Embedded Systems. *IEEE International Conference on Embedded Software and Systems*, 180-187.

Disabling attacks are designed to shut down or interfere with one or more of the AV's systems. Examples include turning off the engine, disrupting the engine's firing timing, or locking the ignition. The severity of the impact depends on when the attack is executed. If the attack happens while the vehicle is stationary, the consequences may be minimal. However, disabling an AV while it is in motion could lead to significant damage or even collisions. Real-world tests have demonstrated similar vulnerabilities in the past[60].

(i) Overprovision of Services Attacks

These attacks force the AV to execute unintended actions, such as sudden acceleration, abrupt braking, or unintended steering. They are analogous to denial-of-service (DoS) attacks commonly seen in cybersecurity, where a system is overwhelmed by multiple requests, causing it to malfunction. Depending on the timing and location, such attacks can result in significant harm, especially in congested or high-speed traffic environments[61].

(ii) Data Manipulation Attacks

Data manipulation attacks alter or erase the data used by the AV to make decisions. For example, manipulating LiDAR data could make the AV fail to detect obstacles or misjudge distances, leading to accidents. This form of attack may also involve tampering with AVs' sensor inputs or using methods like data poisoning, where compromised data fed into machine learning models results in unsafe behavior[62]. Data poisoning could involve subtle changes in physical signs, training datasets, or operational conditions that skew the AV's behavior.

(iii)Data Theft

Data theft involves stealing sensitive user information, such as travel patterns, conversations recorded by onboard microphones, or personal data stored in the AV's cloud systems. Hackers could exploit vulnerabilities in AVs or the data centers that store related information, including those of third-party cloud providers. Similar attacks on consumer data have resulted in large-scale privacy violations[63].

- **Relevant Legal Provisions**

AVs, given their reliance on sophisticated software, communication networks, and sensitive data processing, fall within the scope of the IT Act. The increasing risk of cyberattacks targeting AVs highlights the need for robust legal provisions to hold stakeholders accountable. Below is an expanded analysis of the key sections of the IT Act relevant to AV cybersecurity:

a. Section 43A: Liability for Failure to Protect Data

Section 43A of the IT Act deals with the liability of body corporates for failing to implement "reasonable security practices and procedures" to protect sensitive personal data. This section applies directly to AV manufacturers, service providers, and software developers, as these vehicles process substantial amounts of personal data, including but not limited to location data, travel preferences, and potentially even biometric data for authentication or access control.

The definition of "sensitive personal data" is outlined in the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011, which were framed under Section 43A. Data collected by AVs can fall into this category, particularly if the vehicle's sensors and software track the vehicle's movement, passenger preferences, and other forms of biometric identification (e.g., voice or facial recognition).

[60] Supra 51
[61] Supra 55
[62] Supra 56
[63] Woolley, S. C. (2017). Equifax Breach: Timeline and List of 147 Affected Companies. *Forbes*.

If a manufacturer, developer, or service provider fails to adopt adequate encryption or other cybersecurity measures to protect this data, they may be held liable under Section 43A. For instance, if a cyberattack occurs because of poor encryption protocols, and data such as travel routes or driver authentication credentials are compromised, the AV manufacturer could face penalties and be required to compensate those affected.

While not directly related to AVs, the case of *NASSCOM v. Ajay Sood*[64] set a precedent for liability under Section 43A. The case involved a cybercrime committed by a private entity, and the judgment stressed the need for reasonable security practices to be in place to protect sensitive data. In the context of AVs, this case highlights the importance of manufacturers and developers ensuring that reasonable cybersecurity measures are adopted to avoid similar liabilities.

b. Section 66: Hacking and Unauthorized Access

Section 66 of the IT Act criminalizes hacking, defined as any act of gaining unauthorized access to a computer system or resource. Autonomous vehicles, with their onboard computers and interconnectivity through vehicle-to-infrastructure (V2I) and vehicle-to-vehicle (V2V) communication systems, fall within the purview of "computer resources" under the IT Act. Cyberattacks on these vehicles, whether through exploitation of software vulnerabilities or unauthorized access to the vehicle's systems, may result in both criminal charges under Section 66 and civil liabilities under Section 43A.

While Section 66 primarily targets the perpetrators of hacking, manufacturers and developers may still face liability if their failure to adopt robust cybersecurity protocols facilitates such an attack. If a software developer produces code that contains known vulnerabilities or fails to patch security flaws in a timely manner, they could be held responsible for any resulting damage.

In *Shreya Singhal v. Union of India*[65], while the primary issue was about freedom of speech, the case also shed light on the broad definitions under the IT Act, including how "computer resources" are defined. This case provides a basis for interpreting the IT Act's provisions in the context of AVs, especially when vehicles are compromised through hacking or unauthorized access.

In 2015, researchers demonstrated how they could remotely hack into a Jeep Cherokee's systems, controlling the vehicle's brakes, steering, and transmission. While this event did not occur in India, it highlights the potential consequences of inadequate cybersecurity in AVs.[66] The Jeep Cherokee hack underscores the need for stringent compliance with laws like Section 66 of the IT Act to criminalize such attacks and impose legal obligations on manufacturers and developers to secure their systems.

c. Section 69: Governmental Powers for Cybersecurity

Section 69 of the IT Act grants the government extensive powers to intercept, monitor, or decrypt information for purposes such as national security or to prevent cyber incidents. In the case of autonomous vehicles, which are expected to be integrated into smart city infrastructure, this provision is critical from a cybersecurity standpoint. A cyberattack on AV networks could disrupt essential services, leading to not only individual harm but also wider consequences for public safety and national security.

Given the potential for AVs to serve as critical infrastructure components in smart cities, Section 69 can be invoked to address national security concerns in cases where cyberattacks on AVs could disrupt city-wide transportation systems or public safety mechanisms. While this section empowers the government

[64] NASSCOM v. Ajay Sood, 119 (2005) DLT 596 (India)
[65] Shreya Singhal v. Union of India, (2015) 5 SCC 1 (India)
[66] Andy Greenberg, *Hackers Remotely Kill a Jeep on the Highway—With Me in It*, Wired (July 21, 2015), https://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway/.

to intercept communications in the interest of cybersecurity, it does not mandate specific preventive measures that manufacturers and developers must follow.

In *State v. Navjot Sandhu*[67], also known as the Parliament Attack Case, the Supreme Court interpreted the government's power under Section 69 of the IT Act to intercept and monitor information in cases involving national security. While this case did not involve autonomous vehicles, it demonstrates how Section 69 could be applied to AV cybersecurity if the vehicle systems are used in a manner that threatens national security.

CHAPTER 5 – GAPS IN THE INDIAN LEGAL SYSTEM

As autonomous vehicles (AVs) continue to evolve, India's current legal system remains inadequate to address the complexities that arise in relation to AV accidents, cybersecurity risks, and the allocation of liability among stakeholders. This section examines the shortcomings of key Indian laws, such as the Motor Vehicles Act, 1988, and the Information Technology Act, 2000, while comparing international approaches and highlighting the need for regulatory reform.

I. Inadequacies of the Motor Vehicles Act, 1988

The Motor Vehicles Act, 1988, is the cornerstone of India's road traffic law but was designed with human-driven vehicles in mind. With the advent of AVs, several provisions of the Act become obsolete, particularly when addressing non-human-driven vehicle accidents.

(i) Inability of the Current Act to Cover Non-Human-Driven Vehicle Accidents

Sections 4 and 5 of the Motor Vehicles Act focus exclusively on human drivers, thus failing to account for scenarios where a vehicle operates autonomously without human control. These sections impose duties on licensed drivers, neglecting the role of artificial intelligence (AI) systems as drivers.

- **Section 4 (Driving by unlicensed persons)** prohibits driving by individuals who do not hold a valid driver's license. AVs, particularly at higher levels of automation (Levels 4 and 5), may operate without human intervention, rendering this provision irrelevant. There is no legal recognition of an AI "driver" under this section.
- **Section 5 (Responsibility of owners of motor vehicles for contraventions)** places liability on vehicle owners to ensure their vehicle is driven by a licensed person. In the case of an AV accident, the question arises: Is the owner liable even if they were not controlling the vehicle at the time of the accident? The Act does not address this issue, creating ambiguity around owner liability in fully autonomous driving modes.

(ii) Driver's Role and Liability in AV Accidents

As AVs diminish the role of human drivers, the traditional concept of driver liability becomes increasingly complicated. The Act does not envision scenarios where no human intervention is required. In cases where a human is still present in the AV but not actively controlling the vehicle, courts will need to determine the extent to which the driver is still liable.

In *Millner v. Department of Motor Vehicles*[68], the California courts dealt with a case involving the testing of self-driving vehicles, concluding that the operator of the test vehicle was still responsible for its safety despite the vehicle's autonomous features. Indian courts may adopt a similar approach, but this is speculative given the absence of clear legislative provisions addressing AV-specific liability.

II. Limitations of the Information Technology Act, 2000

[67] State v. Navjot Sandhu, (2005) 1 SCC 130 (India)
[68] Millner v. Dep't of Motor Vehicles, 153 Cal. App. 4th 1354 (Cal. Ct. App. 2006).

While the Information Technology Act, 2000, governs cybercrimes and data protection, it is not sufficiently tailored to address the unique cybersecurity risks posed by AVs. As AVs rely on advanced software, communication networks, and data processing, they are vulnerable to cyberattacks that could have severe consequences, including endangering lives.

(i) Insufficient Engagement with Cybersecurity Risks Posed by AVs

The IT Act provides certain safeguards under Section 43A and Section 66, but these provisions do not specifically address cybersecurity challenges unique to AVs.

- **Section 43A** requires body corporates to implement "reasonable security practices" to protect sensitive personal data. While AVs certainly collect personal and sensitive data (e.g., GPS data, driver biometrics), the definition of "reasonable" remains vague and does not account for the high-security demands of AVs. A study conducted by *Cybersecurity Ventures* estimated that by 2025, AVs will face over 20 million attempted cyberattacks daily, highlighting the critical need for AV-specific security protocols.[69]
- **Section 66** criminalizes hacking and unauthorized access to computer resources. AV systems, which are effectively mobile computer systems, fall under this provision. However, this section only punishes external attackers and does not address situations where manufacturers or developers fail to secure the AV's systems against potential breaches. In *Ratan Lal v. State of Rajasthan*[70], a case concerning hacking, the courts recognized that inadequate cybersecurity measures can have profound legal consequences, but no direct application to AVs has yet been considered.

(ii) Lack of Specific Regulations for AV Technology and Cyberattacks

Cyberattacks on AVs are particularly dangerous, as they could result in remote hijacking of vehicles, traffic disruption, or even fatal accidents. The IT Act does not directly address these types of risks, and the penalties for cybersecurity lapses under the Act may not suffice in such cases.

- In contrast, the European Union's *Cybersecurity Act (2019)*, in conjunction with the *General Data Protection Regulation (GDPR)*, mandates that manufacturers of autonomous systems, including vehicles, must meet high cybersecurity standards. This regulatory framework could serve as a model for India as it considers how to address AV cybersecurity.
- Moreover, the *National Highway Traffic Safety Administration (NHTSA)* in the United States has introduced guidelines for manufacturers of AVs to mitigate cybersecurity risks, including mandatory reporting of any cyber vulnerabilities. In India, no such guidelines exist under the IT Act or other legislation.

III. Stakeholder Liability

In the case of an AV-related accident, liability is no longer confined to the driver or vehicle owner. AV technology introduces multiple stakeholders, including manufacturers, software developers, and operators, all of whom could be held responsible for an accident or system failure. However, current Indian law does not clearly outline how liability should be apportioned among these parties.

Unclear Provisions for Distributing Liability Among Involved Parties in AV-Related Accidents

India's legal system does not provide a clear framework for determining the liability of manufacturers and developers in cases where AV systems malfunction or fail. This gap creates significant uncertainty for all parties involved in an AV-related accident.

[69] *Cybersecurity Ventures, Cybersecurity Market Report* (2020), https://cybersecurityventures.com/research/.
[70] Ratan Lal v. State of Rajasthan, (2010) 3 SCC 201 (India)

- **Strict Liability under the Consumer Protection Act, 2019**: Although the CP Act provides for strict liability against manufacturers for defective products, it does not specifically address defects in autonomous systems or software malfunctions. There is little precedent in Indian courts for dealing with software-related defects in AVs, which will likely lead to litigation in the future.
- **Contractual Liability**: Manufacturers and developers of AVs often include contractual clauses limiting their liability in the event of system failures. However, these clauses may be contested in Indian courts under the *Indian Contract Act, 1872*, particularly if the defect resulted in significant harm or loss of life.

In Product Liability under the CP Act, it is to be noted that while India's product liability regime holds manufacturers accountable for defective goods, software and digital services—key components of AVs—are often overlooked. AV developers may argue that software failures fall outside the ambit of product liability, leaving courts to navigate this uncharted territory.

International Approaches to Stakeholder Liability

In other jurisdictions, comprehensive legal frameworks for AV liability are being established. For example:

- In Germany, AV manufacturers are required to comply with strict safety standards and are held liable for any accidents caused by defects in the vehicle's autonomous system.
- The UK's Automated and Electric Vehicles Act provides a clear division of liability between vehicle manufacturers and insurers, ensuring victims of AV accidents are compensated promptly.

India's lack of specific AV legislation leaves stakeholders uncertain about their legal obligations. Without reform, manufacturers and developers may face inconsistent rulings, leading to prolonged litigation and uncertainty in AV adoption.

CHAPTER 6 – INTERNATIONAL PERSPECTIVES

United Kingdom (UK)

The UK's *Automated and Electric Vehicles Act, 2018 (AEVA)* offers a potential roadmap for India. It extends liability for accidents involving AVs to insurers first, and then allows insurers to recover costs from manufacturers if the AV is proven faulty. This method accommodates the absence of a human driver and recognizes that the AV's technology may bear responsibility for accidents. India currently has no comparable legislation, and without it, the Motor Vehicles Act remains inadequate for AV regulation.

- AEVA's Dual-Layer Liability: The dual-layer liability system (first involving insurers, then manufacturers) mitigates the burden on individuals in navigating the complexities of AV technology. This approach places consumer protection at the forefront while ensuring that manufacturers maintain high standards of safety.
- Strict Product Liability: AEVA implicitly enforces strict product liability on manufacturers if a defect in the AV's system causes an accident. This provides clarity on how manufacturers will be held responsible if a vehicle's automated functions fail.

Section 2 establishes that insurers are liable for damage caused by an AV when it is driving itself. Victims can claim compensation from insurers, who then have the right to recover costs from the manufacturer if the accident was caused by a failure in the vehicle's automated systems. Section 3 excludes liability if the AV is damaged due to unauthorized modifications or failure by the vehicle owner to update the software. Section 4 addresses cases where the insurer can limit liability, such as when the vehicle's software is not updated as required, thus emphasizing the role of manufacturers in issuing timely updates. In case of a system failure, the AEVA allows victims to bypass the complexities of proving fault on part of the AV

manufacturer and instead claim compensation directly from insurers, with the insurer later recovering damages from the manufacturer.

Germany

Germany, a leader in the automotive industry, passed legislation in 2017 that sets forth a legal framework for Level 3 and Level 4 autonomous vehicles. The *German Road Traffic Act (Straßenverkehrsgesetz)* mandates that while autonomous driving is allowed, the human driver remains responsible unless the vehicle is in a fully automated mode. This creates a hybrid approach, where driver liability is retained, but manufacturers can be held liable if an accident occurs when the vehicle is in automated mode.

- Dual-Role of Drivers and Manufacturers: If the AV is in manual or semi-autonomous mode, liability falls on the driver. However, in fully autonomous mode, liability may shift to the manufacturer or software developer, especially if a technical failure occurs. German law also requires manufacturers to install a black-box-like device to log data from the vehicle, ensuring that accidents are properly investigated.
- Legislative Updates: The 2021 amendments further expand the legal basis for fully autonomous driving, including the development of test zones for AVs and clear liability rules for manufacturers in case of system malfunctions.

Section 1b allows for AVs (Level 3 and 4 automation) to operate under certain conditions. It emphasizes that the driver must remain available to take control if necessary, but the manufacturer can be liable if the AV operates in fully autonomous mode. Section 7 stipulates that AVs must have a black box that records data to determine who or what was in control during an accident. The data is crucial in assigning liability. Section 18 expands on liability for AV-related accidents, providing that manufacturers are responsible if an accident occurs during fully autonomous operation, while the driver is liable if they are in control. If an accident occurs while the AV is fully autonomous, liability shifts to the manufacturer, particularly if the failure is due to a defect or a cybersecurity breach.

United States (California)

California has been a frontrunner in the AV space, given its role as a global tech hub. The California Department of Motor Vehicles (DMV) regulates AV testing and deployment, particularly concerning safety and liability. The DMV mandates that manufacturers carry liability insurance or surety bonds worth at least $5 million before they can test AVs on public roads. California law also places liability on AV manufacturers for accidents caused by their technology, shifting responsibility from human drivers to companies.

- AV Testing Regulations: AV manufacturers are required to submit annual reports detailing the safety of their autonomous systems, including disengagements and accidents. In case of an accident, California holds the manufacturer responsible for any damage caused if the AV was operating autonomously at the time.
- Liability for Testing Failures: The *California Autonomous Vehicle Regulations* focus heavily on the safety of testing AVs, imposing strict liability on manufacturers if an accident occurs due to negligence in testing protocols. This contrasts with other jurisdictions where testing environments are less regulated.

Title 13, Section 227.24 requires manufacturers to provide evidence of insurance or surety bonds of at least $5 million before testing AVs on public roads. Section 227.56 specifies that manufacturers must submit annual disengagement reports and accident reports, showing how often human drivers had to take control of the AV. In case of an accident during testing or autonomous operation, manufacturers can be

held liable if the fault lies with the AV system. Section 227.58 governs the testing of AVs without a safety driver, stating that AV manufacturers are strictly liable for damages caused by their vehicles during autonomous operation. If an AV accident occurs due to a cybersecurity breach, manufacturers are liable under California law, provided the AV was operating in autonomous mode at the time.

European Union (EU)

The European Union has been proactive in establishing a legal framework for AVs, although much of the regulation is still under development. The EU's *General Data Protection Regulation (GDPR)* plays a crucial role in managing the personal data collected by AVs. However, liability in the case of accidents is governed by member states' domestic laws, which vary widely. The EU is working toward harmonizing these laws through initiatives such as the *Artificial Intelligence Act* (still in proposal) and *Product Liability Directive*.

- GDPR and Data Protection: GDPR is relevant for AVs because these vehicles collect vast amounts of personal data, including location, biometrics, and behavioral patterns. Under GDPR, manufacturers are responsible for ensuring that personal data collected by AVs is handled according to stringent data protection principles, or face significant penalties.

Article 5 requires that personal data collected by AVs (such as location and biometric data) must be processed lawfully, transparently, and for specified legitimate purposes. Article 32 mandates data controllers (such as AV manufacturers) to implement appropriate technical and organizational measures to ensure data security, including encryption and anonymization, which is particularly relevant for protecting sensitive AV data against cyberattacks. Article 82 provides a right to compensation for individuals who suffer material or non-material damage due to violations of GDPR. In the context of AVs, this could apply to breaches involving personal data stored or transmitted by AVs. Manufacturers are required to comply with data security standards, and any cyberattacks resulting from failure to comply may lead to significant penalties under GDPR.

- Proposed AI Act: The proposed *AI Act* categorizes AVs as high-risk AI systems and imposes strict requirements for safety, transparency, and liability. Manufacturers could face penalties for system failures, similar to product liability under the *Product Liability Directive*.

Chapter 2, Article 6 classifies autonomous driving systems as "high-risk" AI systems and requires rigorous testing, transparency, and documentation before deployment. Article 16 requires manufacturers to implement continuous monitoring systems and report incidents related to their AI, including cybersecurity breaches. Article 70 outlines fines and penalties for non-compliance, with penalties up to €30 million or 6% of global annual turnover for violations involving cybersecurity failures in high-risk AI systems like AVs. If an AV's AI system causes an accident due to a cyberattack or malfunction, the manufacturer could face heavy fines under the AI Act once it is enacted.

Singapore

Singapore has emerged as a global leader in regulating AVs, adopting a proactive, regulatory sandbox approach to testing AVs on public roads. The *Autonomous Vehicles Act, 2019* allows for AV testing and deployment but places strict liability on manufacturers and developers if an accident occurs due to a malfunction in the AV system.

- Regulatory Sandbox Approach: Singapore allows for extensive testing of AVs under real-world conditions, but with legal safeguards in place to protect the public. The *Autonomous Vehicles Act* imposes strict liability on AV operators for accidents that occur due to software or hardware failures.

- Compensation for Victims: In the event of an AV accident, Singapore's system ensures that victims are compensated swiftly by mandating insurance for AV operators. The system allows victims to seek compensation either from the vehicle's operator or the manufacturer if the accident was caused by a malfunction.

Section 9 regulates AV trials and deployment. Operators must have insurance coverage for third-party liability in case of an accident. Section 16 mandates that manufacturers must implement cybersecurity measures to protect AV systems from unauthorized access or hacking. Any breaches leading to accidents may hold manufacturers liable. Section 25 establishes a legal framework for AV accident investigations, allowing the state to investigate and assign liability between the operator and the manufacturer based on the data collected by the AV's systems. If an AV is involved in a cyberattack or system malfunction, the act provides a clear basis for assigning liability to the manufacturer, especially if cybersecurity measures are found to be inadequate

Japan

Japan passed its *Road Transport Vehicle Act* amendment in 2020, which explicitly allows for the commercialization of AVs. Japan's approach to AV liability includes strict product liability for manufacturers and developers, similar to consumer protection laws in Europe. Japan also requires AVs to be equipped with cybersecurity measures to prevent hacking, with manufacturers facing penalties if they fail to secure their systems.

- Product Liability for Defective AV Systems: If an AV is involved in an accident due to a defect in the software or hardware, the manufacturer is held strictly liable under Japan's *Product Liability Act*. This law provides consumers with a direct avenue for seeking compensation from AV developers if an accident occurs.
- Cybersecurity Requirements: Japan mandates that manufacturers adhere to high cybersecurity standards to prevent hacking, with legal provisions for holding companies accountable if a breach results in an AV accident.

Article 9 stipulates that AVs must undergo stringent approval and testing before deployment. Manufacturers are liable for accidents resulting from defects in their software or hardware. Article 42-2 requires that AV manufacturers ensure high levels of cybersecurity and that data from the vehicle be collected and stored securely to prevent cyberattacks. Product Liability Act provides strict product liability for manufacturers whose defective products, including AVs, cause harm. If an AV system fails due to cybersecurity issues, the manufacturer can be held liable under this act. Japan's laws place a clear emphasis on cybersecurity and the responsibility of manufacturers to maintain secure AV systems. If a breach occurs, manufacturers face liability under both the Road Transport Vehicle Act and Product Liability Act.

CHAPTER 7 – RECOMMENDATIONS

Revising the Motor Vehicles Act, 1988

The Motor Vehicles Act (MVA), 1988, as it currently stands, is ill-equipped to deal with the unique challenges posed by autonomous vehicles (AVs). The legal framework focuses on human drivers and does not account for the possibility of accidents caused by machine errors or cyberattacks. Thus, the following amendments are recommended:

- Incorporating AVs into the Liability Framework: Amend the definition of "driver" and "vehicle operator" to explicitly include autonomous vehicles. This would ensure that liability for AV-related

accidents is not constrained to human drivers. Amendments to *Section 4* and *Section 5*, which pertain to the duties of drivers, should extend to "operators" or "controllers" of AV systems.

- Addressing Non-Human Errors: Introduce provisions that allocate liability in cases where an AV operating in autonomous mode causes an accident without human intervention. The framework should:
  - Include strict liability provisions for manufacturers and software developers where defects in AV systems cause harm (*Res ipsa loquitur* principles could be applied to AV malfunctions).
  - Introduce a comprehensive insurance model (similar to the UK's AEVA, 2018), wherein insurers compensate victims and recover damages from AV manufacturers or developers.
- Amending Section 161 (Hit-and-Run Scheme): Update the current hit-and-run compensation provisions to include scenarios where AVs cause accidents without human control. The existing "driver" concept in the scheme does not account for autonomous systems where liability is distributed between various stakeholders.

Enhancing the Information Technology Act, 2000

The Information Technology Act, 2000 (IT Act), is currently the primary legislation governing data protection and cybersecurity, but its scope remains insufficient for addressing the unique risks posed by AVs. The following reforms are necessary:

- Specific Provisions for Cyberattacks on AVs: Introduce a distinct section dedicated to AVs, defining cyberattacks on AV systems as offenses under the IT Act. These offenses should include:
  - Unauthorized access, hacking, and manipulation of AV systems.
  - Manipulation of vehicle-to-infrastructure (V2I) and vehicle-to-vehicle (V2V) communication, both of which are critical for AV functioning.
  - Failure to implement adequate cybersecurity measures should be treated as a distinct offense, allowing authorities to hold manufacturers accountable if a vehicle's system is compromised.
- Strengthening Penalties and Responsibilities: Amend *Section 66* (Hacking) and *Section 43A* (Failure to Protect Data) to include harsher penalties for cybersecurity breaches in AVs. A separate provision for high-risk systems, such as AVs, would ensure that breaches affecting public safety are penalized more severely, similar to the GDPR fines in Europe.
- Mandatory Disclosure Requirements: Enforce mandatory reporting of cybersecurity incidents related to AVs under a newly introduced section akin to *Section 70B* of the IT Act, which governs cybersecurity breach reporting for critical information infrastructure. This would ensure that the government is informed of AV-related breaches and can take preventive measures.

Introducing New Regulatory Frameworks

India's current legal landscape lacks a comprehensive framework tailored specifically for autonomous vehicles. Given the complexities of AV technology, a new regulatory body and set of standards are urgently needed:

- Establishing a Separate AV Regulatory Body: The government should create an independent regulatory body, akin to the *National Highway Traffic Safety Administration (NHTSA)* in the U.S. or the *Centre for Connected and Autonomous Vehicles (CCAV)* in the UK. This body would:
  - Oversee testing, certification, and approval of AV systems.
  - Monitor the performance and safety of AVs operating in India.
  - Investigate accidents involving AVs and help adjudicate liability between manufacturers, software developers, and operators.

- Guidelines for Cybersecurity Standards: The regulatory body should introduce mandatory cybersecurity standards for AV manufacturers and developers, with guidelines that cover:
  - Data encryption, secure communication protocols, and real-time monitoring to protect against cyberattacks.
  - Periodic updates and patches to AV software to address newly discovered vulnerabilities (similar to the *California Autonomous Vehicle Regulations*).
  - A certification process to ensure compliance with cybersecurity standards, as is done under the *ISO 26262* standard for functional safety in road vehicles.
- AV Safety Measures: Propose a set of safety guidelines for AV deployment, including:
  - Black-box data recorders, similar to those mandated under Germany's *Road Traffic Act* (Section 7), which would help in post-accident liability determination.
  - Real-time monitoring of vehicle health and predictive maintenance systems to prevent breakdowns and reduce accidents.
  - Requirements for continuous operator training and involvement to ensure that human controllers can effectively intervene when necessary.

International Inspiration

- Germany: Germany's *Straßenverkehrsgesetz* mandates detailed liability assignments for AV systems, including mandatory black-boxes and cybersecurity standards. India could incorporate similar provisions that address liability distribution among stakeholders.
- UK: The UK's *AEVA* (2018) provides a streamlined compensation model through insurers, protecting victims while allowing insurers to recover damages from manufacturers in cases of AV malfunction. India's insurance framework could be expanded to allow similar recovery models.
- California: The *California Autonomous Vehicle Regulations* require detailed reporting on AV system disengagements and accidents. Introducing similar reporting requirements in India would promote transparency and accountability in the event of system failures or cyberattacks.

CHAPTER 8 – SUGGESTED LIABILITY FRAMEWORK

In the context of AV accidents caused by cyberattacks, liability must be distributed across multiple stakeholders including manufacturers, software developers, network service providers, and vehicle owners, based on a deeper understanding of cyber vulnerabilities, responsibility for mitigating risks, and the principle of fairness. Given the novel risks posed by such attacks, the existing legal system in India (such as the Motor Vehicles Act, IT Act, and cybercrime frameworks) does not adequately address liability distribution in this space. Hence, we need a comprehensive, multi-tiered liability regime.

- **Proposed Framework: "Tiers of Responsibility" Approach**

This approach suggests a tiered structure to assign liability based on the nature of the cyberattack, the degree of control, and the preventive measures implemented by each party involved. The key tiers are:

Tier 1: Manufacturer & Software Developer Liability

- **Primary Responsibility**: This tier covers manufacturers and software developers (both of the AV system and cybersecurity features) and assigns strict liability for any cybersecurity failures related to system design or software vulnerabilities that were foreseeable or preventable.
- **Requirement**: Mandatory security by design requirements should be enforced, ensuring cybersecurity is built into both hardware and software.

- **Liability Trigger**: If a cyberattack exploits a known vulnerability in the AVs hardware or an unpatched software issue and the manufacturers or developers failed to address or mitigate the risk, they bear full liability for the consequences of the accident. This includes failure to implement security-by-design principles or failure to release timely patches/updates for known cybersecurity threats. This also extends to vehicle-to-vehicle (V2V) and vehicle-to-infrastructure (V2I) communications systems.
- **Liability Type**:
  - **Strict Liability** – Manufacturers and developers are liable for any harm caused by defects in software or hardware that could have been prevented by reasonable cybersecurity measures.
  - **Shared Liability**: If the cyberattack is a sophisticated, unforeseen event that exploits an unknown vulnerability, liability may be shared with network providers and vehicle owners who fail to meet their own responsibilities (see below).

Tier 2: Network Provider & Data Processor Liability

- **Shared Responsibility**: This tier holds network providers and cloud service providers accountable for their role in enabling AV operations, particularly in terms of data processing, real-time connectivity, and ensuring secure data transmission.
- **Requirement**: They must meet strict data protection standards and cyber hygiene practices, as well as secure the communication infrastructure.
- **Liability Trigger**: A breach in data integrity or a failure in protecting sensitive data (e.g., vehicle location, driver preferences, or navigation data) that leads to the attack will place shared liability on network providers and data processors. The cyberattack results from a failure in secure communication infrastructure, such as a data breach, insecure vehicle-to-vehicle (V2V) or vehicle-to-infrastructure (V2I) systems, or if there's a failure in protecting the data being processed or transmitted.
- **Liability Type**:
  - **Negligence-Based Liability** – Network providers and data processors are liable if they fail to meet the established data protection or cybersecurity standards for AVs.
  - **Shared Liability**: If the data breach or communication breakdown occurred due to a joint failure (e.g., improper patching by the manufacturer or negligence on the part of the vehicle owner in applying updates), liability is shared with manufacturers and owners.

Tier 3: Vehicle Owner & User Responsibility

- **Limited Responsibility**: While AV owners do not have control over software design, they are responsible for ensuring that the software updates and security patches provided by manufacturers are implemented.
- **Requirement**: Vehicle owners must adhere to periodic maintenance and patch updates, as stipulated by the manufacturer.
- **Liability Trigger**: The vehicle owner fails to install software updates, security patches, or perform necessary maintenance as recommended by the manufacturer, allowing a cyberattack to occur due to outdated or vulnerable software. If the AV accident results from failure to update security patches, partial liability is imposed on the owner, reflecting their negligence in maintaining the vehicle's cyber defenses.
- **Liability Type**:
  - **Negligence-Based Liability** – The owner is liable for not taking reasonable steps to keep the AV system secure by neglecting to follow manufacturer instructions or updates.

- **Shared Liability**: Liability is shared with the manufacturer if the manufacturer failed to provide timely and adequate security updates, or with network providers if the attack also exploited network vulnerabilities.

Tier 4: Government and Regulatory Oversight

- **Regulatory Responsibility**: Governments should enact and enforce cybersecurity and safety standards for AVs, ensuring a baseline level of security for consumers.
- **Requirement**: A dedicated regulatory framework governing cybersecurity standard for autonomous vehicles should be created, with oversight from bodies such as the National Highway Authority of India (NHAI) and the Indian Computer Emergency Response Team (CERT-In).
- **Liability Trigger**: A regulatory body fails to enforce minimum cybersecurity standards or fails to conduct proper oversight on AV security protocols, leading to an environment where cyberattacks are more likely or remain unaddressed. If a government failure in regulatory oversight or certification leads to a safety gap that contributed to the cyberattack, a portion of the liability may rest with the state, particularly where lack of enforcement or poor regulatory standards enabled the attack.
- **Liability Type**:
  - **Partial Government Liability** – Regulatory bodies could be partially liable if their negligence or failure to enforce or update cybersecurity standards contributed to the accident.
  - **Shared Liability**: Government liability may be shared with manufacturers, developers, and network providers if multiple parties failed to meet cybersecurity standards.

When Liability Should Be Shared

1. **Combined Failures (Shared Liability)**:
   When an accident occurs due to a combination of factors, such as:
   - A manufacturer's failure to release patches and the vehicle owner's failure to install those patches.
   - A network provider's failure to secure communications coupled with data processing vulnerabilities in the AV. In these cases, liability should be proportionally shared based on the degree of fault attributed to each party, with manufacturers and developers generally bearing a larger share due to their role in security-by-design.
2. **Sophisticated Cyberattacks (Shared or Limited Liability)**:
   In cases of advanced cyberattacks (e.g., state-sponsored or highly sophisticated attacks exploiting zero-day vulnerabilities), liability may be mitigated or shared:
   - **Mitigated for manufacturers or network providers** if reasonable, industry-standard cybersecurity practices were followed, and the attack was not foreseeable.
   - **Shared with government regulators** if it is determined that their failure to enforce cybersecurity standards or lag in regulatory action contributed to the vulnerability.
3. **Joint Deficiencies in Multiple Layers (Shared Liability)**:
   When both hardware/software vulnerabilities and network infrastructure flaws are exploited simultaneously in a cyberattack, both manufacturers/developers and network providers share responsibility. Additionally, vehicle owners may share liability if they failed to update or maintain the vehicle's security systems in line with manufacturer recommendations.

CHAPTER 9 – CONCLUSION

The evolution of AVs represents a pivotal moment in transportation technology, offering the potential to enhance safety, convenience, and innovation. However, these advancements also introduce complex legal

challenges, particularly concerning liability in the event of accidents caused by cyberattacks. The existing legal frameworks in India, including the Motor Vehicles Act, 1988 and the Information Technology Act, 2000, fall short of adequately addressing these challenges, particularly when it comes to the allocation of liability and addressing cybersecurity threats.

India's Motor Vehicles Act, 1988, while robust in many respects, was not designed to address the complexities of non-human-driven vehicles. Key concepts such as driver responsibility, negligence, and liability need to be reconsidered in the context of AV technology. Current provisions fall short in accounting for incidents where AV malfunctions or system failures, rather than human error, are the primary cause of accidents. Revising the Act to integrate AVs into the liability framework is critical, especially in delineating responsibility among manufacturers, developers, and operators.

On the cybersecurity front, the Information Technology Act, 2000, while providing a foundation for addressing cybercrimes, lacks the specificity required to address the unique risks posed by AVs. With AVs relying heavily on data processing, real-time connectivity, and AI-driven decision-making, the potential for cyberattacks and unauthorized access creates serious safety and privacy concerns. Strengthening the IT Act to introduce AV-specific provisions, enhanced penalties, and mandatory disclosure of cybersecurity breaches is essential in mitigating these risks.

To bridge these gaps, this paper proposes a multi-tiered liability framework—the "Tiers of Responsibility" approach—which distributes liability across stakeholders, including manufacturers, software developers, network service providers, and vehicle owners, based on their respective roles and responsibilities in mitigating cyber risks. Under this approach:

- **Tier 1** assigns strict liability to manufacturers and software developers for cybersecurity failures in system design or software vulnerabilities, emphasizing the need for security-by-design requirements.
- **Tier 2** holds network providers accountable for secure communication infrastructure and data protection, sharing liability when communication breakdowns contribute to cyberattacks.
- **Tier 3** places responsibility on vehicle owners to ensure timely software updates and system maintenance, imposing negligence-based liability when failure to comply leads to vulnerabilities.
- **Tier 4** involves government oversight, proposing that regulatory bodies could share liability if their failure to enforce cybersecurity standards contributes to an attack.

This liability framework introduces a nuanced approach to assigning responsibility in AV-related accidents, taking into account the multifaceted nature of cybersecurity threats in the AV ecosystem.

India's Motor Vehicles Act needs significant amendments to integrate AVs into the liability regime, considering the shift from human-driven to autonomous systems. The role of human drivers is gradually diminishing, and new mechanisms to address non-human errors in accidents are essential. Simultaneously, the Information Technology Act should incorporate specific provisions that address the cybersecurity risks unique to AVs, with strengthened penalties and clearly defined responsibilities for failures.

In addition to revising existing laws, the creation of a dedicated regulatory body focused on AV technology and cybersecurity is vital. This body could oversee the establishment of cybersecurity standards, investigate cyberattack incidents, and coordinate with industry stakeholders to ensure AV safety and security. International legal frameworks, such as the UK's Automated and Electric Vehicles Act, 2018 and Germany's Road Traffic Act, 2017, offer valuable insights for India's regulatory development. These frameworks underscore the importance of clear liability assignments, comprehensive insurance models, and the need for stringent cybersecurity standards. Additionally, models like the California Autonomous

Vehicle Regulations provide a roadmap for transparency and accountability in AV operations, particularly through mandatory reporting and safety monitoring.

The successful adoption of AVs in India requires not just technological advancements but also a robust legal framework capable of addressing the novel risks posed by this technology. By implementing a comprehensive liability framework, revising current legislation, and enhancing regulatory oversight, India can ensure both the safety of its citizens and the continued development of AV technology. The proposed "Tiers of Responsibility" approach serves as a blueprint for how liability can be effectively distributed among various stakeholders in the event of AV-related cyberattacks, fostering a balanced and fair approach to accountability in this rapidly evolving sector.