Cyber Attacks on Autonomous Vehicles and the Adequacy of India's Legal Framework

AnanthikaG.P[1], Dhanashree R[2]
[1,2]*Fifth Year, B. Com. LL. B, School of Law, SASTRA Deemed University, Thanjavur, Tamil Nadu, India.*

***Abstract*— Artificial intelligence (AI) and complex interconnected system enable autonomous vehicle (AVs) which are transforming international transportation. However, their implementation in India is still in its infancy and it is limited by legal infrastructure and technical issues. This research frames AVs are sophisticated computer networks and cyber physical system which falls under definition of computer, computer network, computer system and resources stated in Section 2(1)(i), 2(1)(j), 2(1)(k) and 2(1)(l) of Information technology Act of 2000. Continuous data exchange facilitates navigation, hazard identification and traffic control and also makes AVs vulnerable to cyber threats like remote hacking, unauthorized access and misuse of operational or personal information. This research integrates the effectiveness of India's existing legal framework in IT Act 2000 and DPDP Act 2023 handling cyber security and data privacy issues. Best practices and new regulatory trends are highlighted from countries like US and EUframework including NHTSA's safety standards and GDPR data protection principles. The need for robust legal and technical protections such as secures software development, intrusion detection and prevention system are underscored by numerous AV cyber security incidents. This study ultimately argues that India does not need a new AV- specific legislation; instead, it requires a limited amendment under Section 43A and Section 70B IT Act, enhanced cyber resilience measures and a need for implementation of AIS 189 guidelines which currently remain non-mandatory and lack binding certification timelines and safety-disclosure obligations.**

***Index Terms*— Autonomous vehicle, AIS 189, Cyber security, IT Act 2000**

I. HISTORICAL BACKGROUND

Automated vehicles have gradually developed from simple mechanical system into highly networked devices. This development led to automation and connectivity but also increased the risk of cyber-attacks. Experiments for autonomous vehicle started during 1920's. In the 1980's early version of self-driving cars was made by Navlab at Carnegie Mellon and Eureka PROMETHEUS at Mercedes- Benz There was only minimal network exposure and attackers need physical access to control them. Majority of cars were mechanical devices with separate electronic control. Bosch created the CAN bus in the 1980's to allow communication between electronic control units (ECUs) in vehicle. This invention set the stage for future networked cyberthreats. SAE defines there are 5 levels of automation beginning from level 0 to level 5. During 1980's vehicles were at SAE level 0 Automation that is driver has full control of all driving task. In 2000 Vehicles started to include wireless interface and remote services. In 2004 and 2007 there was development of autonomous software and sensor fusion (LiDAR, Radar, GPS). Consumer begins to use Bluetooth and GPS for easy navigation and reached Level 1-2 automation provides certain feature like adaptive cruise control and lane keeping but the safety depends on human and these systems are classified as driver assistance. Between 2010 and 2020 vehicles adopted cloud computing for map synchronization, while over the air updates allowed for remote vehicle software enhancements. For increased safety and cooperation V2X (Vehicle to everything) communication enable vehicles to communicate with pedestrians, infrastructure and other vehicles.Such Automation reached Level 3 and 4, and at level 3 system would be taken complete control in certain circumstances and drivers should be ready to intervene whenever it is necessary. Level 4 enabled fully autonomous vehicle in certain areas like highways or geo fenced zones without requiring human driver at all while in use. Around 2020 there was integration of AI where rule-based software that followed fixed instructions to advance AI model that analyzesensor

data. In order to safeguard these AI driven system against cyber threats authorities started to incorporate certain standards to protect from cyber threats. Level 5 automation is now emerging where vehicle can operate independently without any human assistance. At present cars are dependent on software, AI driven system and cloud services and it gets close to Automation level 4 and 5 which increases cyber-attacks and result in actual bodily harm. India is currently in the development stage of level 4 autonomous vehicle.

II. LITERATURE REVIEW

1. "Exploring Legal Liability in the Age of Autonomous Vehicles and Addressing Cyber-attack Risks Under Indian Law (2024)" by Ramachandra Subramanian, IJFMR Vol 6, Issue 6.
This paper examines the deficiencies in India's legal framework regarding liability and cyber security in autonomous vehicle (AV) operations. It highlights that while the Information Technology Act, 2000 and the Motor Vehicles Act, 1988 provide limited coverage for cyber incidents and accidents, they do not adequately address issues arising from autonomous decision-making systems. This paper demands for specific AV legislation and clearer liability distribution among manufacturers, software developers, and users. However, it largely focuses on doctrinal gaps without addressing emerging regulations like ARAI's Draft AIS-189 or international standards such as ISO/SAE 21434, indicating a need for further research to align India's AV governance with global cyber security standards.

2. "Privacy and Data Protection in the Age of Autonomous Vehicles" (2024) by Aarishti Singh,IJFMR, Vol 6, Issue 2
This paper examines the challenges of data privacy and protection concerning autonomous vehicles (AVs) in India. It identifies the vulnerabilities related to vehicle-generated data and highlights the inadequacy of existing Indian laws, such as the Information Technology Act, 2000, and the Digital Personal Data Protection Act, 2023, in addressing AV-specific data security risks. By comparing global privacy frameworks, it emphasizes India's lack of AV-centric data governance and the urgent need for regulatory reform to establish robust data protection standards for the AV ecosystem.

3."Liability of Self-Driving Cars: Challenges and Prospects in the Era of Autonomous Vehicles, inFuturistic Trends in Social Sciences" (2024) byMuchalaAadhisha&Palisetty Yashoda Sai Sri, IIP Series, Vol. 3, Book 22, Ch. 12.
This paper examines the evolving liability challenges posed by autonomous vehicles, emphasizing ethical issues, product liability, and comparative legal approaches across jurisdictions. Their study highlights the absence of clear accountability between manufacturers, software developers, and operators but primarily addresses regulatory and moral dimensions. However, the paper fails to focus on cybersecurity vulnerabilities, data protection obligations, and the legal implications of cyber-attackson autonomous vehicle systems. It also lacks analysis of how existing statutes such as the Information Technology Act, 2000 ortheDigital Personal Data Protection Act, 2023 could be interpreted to address such threats in the Indian context.

4."The Future of Autonomous Vehicles in India: Legal Challenges in Liability, Regulation, and Infrastructure" (2024) by Dibakar Dam, Lawful Legal
This paper examines the promise of autonomous vehicles (AVs) in India improved safety, mobility and efficiency, yet identifies major legal and infrastructural hurdles. It emphasises difficulties in apportioning liability in AV-related accidents under current Indian law, the absence of a comprehensive regulatory regime and the need to upgrade road and digital infrastructure for safe deployment. Comparing to international models, it proposes a risk-based regulatory approach, remote-identification/tracking systems, geofencing and public-private partnerships to foster a sustainable AV ecosystem in India. However, the paper does not adequately engage with cyber-attack risks or the liability implications of software/network failures in AVs an omission that leaves a significant gap in understanding AV vulnerability and accountability and fails to discuss about emerging regulation in India such as ARAI's Draft AIS-189.

III. RESEARCH PROBLEM

With the rapid advancement and deployment of autonomous vehicles (AVs), ensuring robust cybersecurity to protect against increasingly sophisticated cyber threats is critical. This research investigates whether the existing Indian legal and regulatory framework, including the IT Act and AIS 189 cybersecurity standards, is adequate to address these challenges

IV. RESEARCH OBJECTIVE

1. To examine the jurisprudential foundation and legal recognition of autonomous vehicles under Indian law.
2. To analyze the nature and impact of cyberattacks targeting autonomous vehicle systems and their implications for public safety and data protection.
3. To evaluate the applicability and interpretative scope of the Information Technology Act, 2000 and the Digital Personal Data Protection Act, 2023 in governing cybersecurity and liability issues in AVs.
4. To identify the existing legal and regulatory gaps in addressing AV-related cyber offences in India.
5. To study how international frameworks, such as the U.S. NHTSA safety standards and the European Union's Regulation, GDPR, regulate AV cyber security and data privacy.

V. RESEARCH QUESTION

1. To what extent can the existing Indian legal framework, particularly the Information Technology Act, 2000 and the Digital Personal Data Protection Act, 2023, be interpreted to regulate cyber security threats and assign liability in cases of cyber-attacks on autonomous vehicles?
2. How can liability be effectively attributed to manufacturers, software developers, and data processors when a cyber-attack compromises an autonomous vehicle's system or data?
3. What legal reforms or regulatory mechanisms are necessary to establish a comprehensive framework for cybersecurity and liability in autonomous vehicle operations in India?
4. How does the non-mandatory nature of Draft AIS-189—especially the lack of binding timelines, certification requirements, and safety-disclosure obligations—affect India's preparedness for autonomous-vehicle deployment?

VI. SCOPE AND LIMITATION OF STUDY

This study examines the Indian legal framework governing cybersecurity and liability in autonomous vehicles, focusing on the applicability of the Information Technology Act, 2000, and the Digital Personal Data Protection Act, 2023. It also considers the role of emerging standards such as AIS-189 in shaping sector-specific cybersecurity requirements. A brief comparative review of international models is included to identify gaps and suggest improvements for India's regulatory readiness.

This study is confined to the legal and regulatory aspects of cybersecurity and liability in autonomous vehicles and does not examine the technical or engineering dimensions of AV systems. The absence of specific legislation, judicial precedent, and empirical data on AV-related cyber incidents in India limits the practical validation of conclusions. As policy frameworks and technology continue to evolve, the analysis remains primarily doctrinal and interpretative in nature.

VII. RESEARCH METHODOLOGY

This research employs a doctrinal and analytical legal research method, as it relying on existing legal framework including the IT Act, 2000, the DPDP Act, 2023, and the DPDP Rules 2025, along with relevant case law. It critically analyses how the existing legal provision extends to AVs. This study adopts a comparative qualitative approach by examining global model, including EU's ETSC guidelines, GDPR principles, AV Regulations and the U.S. NHTSA framework.This analysis is reinforced by real world cyber security case studies, including the Jeep Cherokee hack in 2015 and cruise AV incident in 2023.

VIII. INTRODUCTION

The term Autonomous vehicle refers to any vehicle capable of performing some or all of its driving tasks without human intervention by utilizing cameras, sensors, and software to understand its surrounding environment and monitor functions like steering,

braking, throttle, and acceleration, thereby handling fallback responsibilities for performing a dynamic driving task. Autonomous vehicles encompass a diverse range of systems, from entirely driverless "self-driving carsto driver-assistance technologies, with different level of standards from Level 0 (fullymanual) to Level 5(fullyautonomous) defined by the Society of Automotive Engineers (SAE). At present World-wide, transportation systems are swiftly progressing towards autonomous mobility, specifically towards Level 4 automation, where vehicles can operate with no human intervention in geofenced areas. Countries such as the United States, United Kingdom,European unionand few other countries have already introduced driverless vehicles into their transportation networks. For instance, companies like Waymo,Tesla,Oxa have launched robotaxi services that operate within geofenced areas. India is making a steady progress in implementing an autonomous vehicle and it is prepared to launch its first ever robotaxi in major cities like Bangalore, Delhi, Hyderabad and Mumbai with technical assistance of Tata Elix and Olo electric and the pilot project begins by end of October 2025. In addition, a Bangalore based startup company is set to launch a driverless vehicle Minus zero Z-pod and the tests are under process and the OLA electric is set to launch the first ever driverless scooter named "Ola solo" expectedly by November 2025. Similarly, India is poised to introduce a multitude of autonomous vehicles. These initiatives reflect India's increased involvement in global transition towards intelligent and self-driving transportation system.

Autonomous vehicle has the ability to revolutionize transportation by reducing traffic, accidents, and even human error. However, the use of autonomous vehicles (AVs) presents serious safety concerns and cybersecurity issues. For example, an attackers may by injecting false signals, mislead a vehicle's LIDAR system by makingit to detectan object which is not inexistence, such as pedestrians or other cars and thereby causing sudden brakes or collisions.Researchers at the University of California experimented with "fake object injection" assaults on first-generation LIDAR systems, demonstrating how easily autonomous vehicles could be misled by manipulated sensor data. These studies, highlighted the need for effective regulatory measures. In this context, India's existing legal frameworks—particularly the Information Technology Act, 2000 and the Digital Personal Data Protection Act, 2023—may suitably beinterpreted to include autonomous vehiclesby broadening their scope to address the cybersecurity risks such as data protection, hacking, and system manipulation that areparticular to AVs and enable India to regulate autonomous vehicles effectively.

IX. LEGAL JURISPRUDENCE OF AUTONOMOUS VEHICLES IN THE CONTEXT OF CYBER-ATTACKS

The jurisprudential aspect of autonomous vehicles raises fundamental questions about the nature of legal responsibility, rights , ownership, possession, property, in an era where decision-making shifts from humans to machines.

1. Rights and Duties

i. Rights

Rights of data principal (vehicle users) has been mentioned under section 11 to 15 DPDP Act, 2023.

The data principals are provided with following rights and duties under this section,

- Right to obtain information as to processing of data (section 11)
- Right to correction and erasure of personal data (section 12)
- Right to grievance redressal (section 13)
- Duty to provide an accurate and authentic information. (section 15)

Rule 13 of DPDP rules,2025 ensures that data principals can exercise their rights by easily access, erase, or manage their personal data through clear options provided on a website of a company or an app. In the case of autonomous vehicles, like robotaxi that collects passenger identification data, audio -video recordings, location and route history this section be applied and the operators must provide a platform like a website or an app where passengers can access, review or erase their data and raise grievance if any regarding its use.

ii. Duties

a) Vehicle manufacturer

In the autonomous vehicle ecosystem, the manufacturer acts as a data fiduciary, collecting data from the data principal (vehicle owner) for lawful

purposes such as vehicle safety, diagnostics, and performance optimization. The manufacturer also collects data to monitor and evaluate the vehicle's performance, ensuring efficiency and reliability. As Original Equipment Manufacturers (OEMs), they have a legal duty to handle this data responsibly under the Digital Personal Data Protection Act, 2023, adopting a robust privacy framework based on Process, People, Technology, and Governance (PPTG). This framework ensures data minimization, user consent and secure third-party data sharing, protecting personal and vehicular data from misuse or unauthorized access. The key idea is that manufacturers must not only maintain data integrity but also ensure lawful, fair, and transparent processing of personal data. Failure to uphold these duties may amount to breach of statutory responsibility, especially in cases of cyber-attacks or data compromise. Thus, maintaining data integrity and privacy compliance forms a core part of the manufacturer's standard of care in AV cybersecurity

Vehicle manufacturers as Data fiduciary have certain duties mentioned under Section 8 DPDP Act 2023

Duties of fiduciary (Section 8)

The essential duties to be followed by data fiduciaries are laid down under section 8 of (DPDP) act. Duties include, fair, lawful, transparent handling of personal data to ensure the data is collected used only for specified purpose. They must ensure the data is accurate, complete, collected for necessary purposes protect it from unauthorized access. The data fiduciary shall erase the data or cause its data processor to erase upon the withdrawal of consent by data principal or when it no longer be useful. Additionally, the data fiduciaries must establish grievance redressal procedure in case of data breach and notify the data protection board and the data principals affected.

A Data Fiduciary shall protect personal data in its possession or under its control, including in respect of any processing undertaken by it or on its behalf by a Data Processor, by taking reasonable security safeguards to prevent personal data breach.

In context of an autonomous vehicle the data fiduciary must clearly specify the purpose behind the collection of data and shall delete the data once the consent is withdrawn or no longer useful.

Rule 6 of DPDP Rules, 2025 provides for a reasonable security safeguard to be adopted to prevent personal data breach. In case of an autonomous vehicle the rule 6 stipulates for encryption of personal data.

b) Software developer

Software developers play a key role in the autonomous vehicle ecosystem by designing and maintaining the systems that enable perception, navigation and decision-making. Autonomous vehicle relies on variety of technology, including machine learning to interpret and respond to environment. Software developers work on integrating these technologies into cohesive system that enable vehicles to make decision, navigation safely and communicate with other vehicles. Their main duty is to ensure that the software remains secure, reliable, and protected from cyber threats. As part of data processing, they share responsibility with manufacturers to maintain data integrity and system safety under the IT Act, 2000 and DPDP Act, 2023. Developers must use secure coding, encryption, and regular system checks to prevent unauthorized access or data misuse.Software developers act as the technical backbone of autonomous vehicles, carrying a duty to protect both system performance and user data.

c) Cloud service provider:

Cloud systems store sensitive AV data such as location, route history, sensor outputs, camera images, user identity, behavior patterns, and even payment details. This collected data helps vehicles learn from each other, improve maps, update software, and offer smoother user services. Because they handle such personal and technical information, cloud providers have a duty to secure it through encryption, access controls, and safe data-sharing practices. They must also maintain strong authentication, regular security checks, and proper storage systems. If they fail in these duties, the data becomes vulnerable to hacking, theft, ransomware, insider misuse, or even remote manipulation of vehicles. Any breach can make the cloud provider legally liable for exposing personal data or compromising passenger safety.

d) Network service provider:

A network service provider (NSP) is essential for autonomous vehicles, giving each car constant, fast, and secure connectivity, usually through networks like 5G. Vehicles rely on this network to receive map updates, accident alerts, or information about

obstacles, which helps them make safe driving decisions like rerouting or slowing down. If a car detects a new danger, the NSP helps send that alert to other vehicles and servers so everyone stays informed. The NSP's duties go beyond just providing internet they must ensure uninterrupted connections, very low delays, strong security, and smooth handovers between networks so AVs never lose contact while moving. Without these duties, autonomous vehicles could not operate safely or stay updated with real-time road information

2. Ownership and Possession

In autonomous vehicle, data ownership and possessionare primarily controlled by manufacturers throughcopyrighted proprietary software, protected under the Digital Millennium Copyright Act (DMCA), which prohibits users from bypassing or "hacking" these systems under its anti-circumvention rule, even if the data originates from their own vehicle. Car owners only receive a license to use the software, and by accepting the End User License Agreement (EULA), they often waive their rights to access or modify in-vehicle data. The case Davidson & Associates v. Jung (2005) reinforces this, holding that users who bypassed software protections despite agreeing to EULA terms violated the DMCA. In the context of autonomous vehicles, this means that owners or technicians who attempt to access or alter software or data without authorization could face similar liability

3.Property:

In autonomous vehicles, the car itself and its hardware parts like sensors, cameras, and computers are considered property and can be owned. The software that runs the vehicle is protected as a literary work under Indian Copyright Act Section 2(o). In the strict legal sense, while core elements of AVs such as the physical vehicle, embedded hardware, and intellectual property like patented algorithms or software are clearly recognized as property under Indian law, raw data generated by AVs is not. Instead, such data is treated as personal data when it relates to an identifiable individual and is regulated by the Digital Personal Data Protection Act 2023, which grants rights of use, consent, and control but does not create ownership rights. Therefore, although the tangible and intellectual components of AVs are protected as property, the data they produce is governed by data protection laws.

X. LIABILITY

The level 4 autonomous vehicles operate without human intervention, as the control decreases the liability for the driver decreases and it is shift towards the vehicle manufacturers, software developer, cloud service provider and network service providers.

Manufacturer developer:

The manufacturer shall be strictly liable for any designs, manufacturing defect including the failure to update the software. Liability may further be evaluated using the reasonable human driver and reasonable computer driver standards, where the autonomous system's behavior is assessed against what a competent human driver would have done or against an industry-accepted technological benchmark. If the vehicle's performance falls below these expected standards, the manufacturer will be liable for the resulting damages. Thus, it can be said that the manufacturer holds the primary responsibility, remains the central accountable party for defects or failures

Software developer:

Autonomous vehicles heavily depend on software to make driving decisions. If an accident occurs due to a software glitch, faulty code, or errors in decision-making algorithms, the software developer—including third-party companies responsible for designing, updating, or maintaining the vehicle's operating system—may be held liable. However, as the primary product provider, the manufacturer initially bears responsibility under product liability law and must investigate the source of the defect. When the malfunction is traced to third-party software and negligence or breach of technical specifications by the developer is established, the manufacturer can pursue indemnification claims against the software developer. This creates a chain of accountability linking the manufacturer's overarching product responsibility with the developer's duty to ensure the safety and reliability of their software components

Liability of Network and Cloud Service Providers as Intermediaries

Network Service Providers and Cloud Service Providers both fall under the category of

"intermediaries" under section 2(1)(w) of IT Act. NSPs enable AVs to connect with external systems, while CSPs store and process AV-generated data. Both enjoy safe-harbour protection under Section 79, but only if they follow due-diligence duties such as securing data, preventing unauthorized access, and acting promptly on breach notifications. Their liability is secondary. They are held responsible only when they alter data, ignore warnings, fails to maintain cybersecurity standards, or violate data-protection obligations, which results in the loss of intermediary immunity. Further, Section 72A also applies, making them directly liable if they knowingly disclose personal information or misuse, it for unlawful gain or cause wrongful loss

Autonomous vehicle security relies on the resilience of interrelated systems, including sensor communication system, software and AI models. Cyber-attacks endanger safety, privacy and confidence in autonomous mobility by taking advantage of flow in these layers. These attacks can be classified into 4 layers such as Sensor level attacks, in vehicle (CAN) attacks, software and remote attacks and adversarial attacks on Machine learning perception.

1. Sensor level Attacks

Sensor level attacks directly target the perception and localization system of AV vehicle s which are essential for safe navigation and environmental awareness. These systems include camera, LiDAR, radar, ultrasonic and GNSS sensors.

i. GPS / GNSS Spoofing and Jamming

Autonomous vehicle's reliance on GNSS and GPS for positioning, navigating and timing exposes them to spoofing and jamming attacks that can mislead vehicle localization. Spoofing is the practice of sending fake satellite signals to deceive a vehicle's GNSS receiver, which leads to inaccurate positioning or time. Jamming disrupts navigation through radio frequency interference by obstructing signals and triggering into emergency mode.

Example- By spoofing GPS signals it makes Tesla's autopilot to follow a wrong navigation path.

ii. LiDAR spoofing and point cloud injection

LiDAR an essential perception sensor for autonomous vehicle, uses laser pulses to create a 3D point cloud of the surroundings. Spoofing occurs when hackers alter the data to mislead the car's perception system into detecting nonexistent obstacle leading to erratic decision making occurs accident.

Point cloud injection is an advanced attack where attackers inject falsified data points into LiDAR's Output creating a believable 3D object using sensor fusion algorithms, despite multiple sensor's confirmation.

Example- In 2015 researchers used a laser device to send back 200 fake reflection points into car's LiDAR,which appeared as false objection in the 3D map. This attack could cause sudden brake and change lanes without any reason.

2. In- vehicle Network (CAN) Attacks

i. Replay attacks

Unexpected car actions can result from replay attacks, which intercept and record CAN messages from vehicle ECU's and cause certain unauthorized actions like unlocking doors or applying brakes.

ii. Denial of service on CAN

Denial of service attacks on car's internal network stop valid ECU message from delivered which results in missing of safety critical signals. This can leads to missed commands,sensor fusion inputs, warning and temporary loss of control.

Example- In Jeep Cherokee hack case 2015, Hackers who remotely accessed its infotainment system, gained access to internal CAN bus and then it flooded the bus with vehicle (DOS) and temporarily blocks communication.

iii. Diagnostic Interface Exploits (OBD IIPorts)

Every car contains diagnostic interfaces such as OBD-II port for maintenance and repairs. Attackers with physical access can plug into these ports and execute direct CAN injection using specialized hardware.

3. Software and Remote attacks

i. Deep fake and synthetic data attacks

Autonomous vehicle can be deceived by malicious actor using deep fakes and synthetic sensor data. Deep fakes can project manipulated imagery. Eg- Showing empty road when there is an obstacle in the road

Whereas synthetic data attacks involve injecting or alter the environmental perception, leading to Phantom objects or masking actual hazards

ii. Mobile app and API Hijacking

Mobile apps and cloud API allows the user to enable remote vehicle management such as unlocking the

doors, starting engines, tracking locations which exposes significant risk

Example- In 2022 Researchers discovered serious vulnerabilities in the Hyundai and Genesis remote access app ‘s API. This enabled an attacker to remotely unlock, start and operate vehicles made after 2012 and takes remote control without the owner’s consent.

4. Adversarial attacks on Machine Learning (ML) perception

a. Digital Adversarial

Adversarial attacks often involve pixel level changes alter images or sensor data which is undetectable and causes misclassification in machine learning models. Example – Attackers have digitally altered images of stop signs by adding minor perturbations and leads to neutral network perceive it as speed limit rather than stop sign.

b. Data Falsification in ML outputs

Data falsification attacks manipulate the AI input, affects both visual and other perception channels like V2X messages, Radar etc. Attackers can modify V2X communications and gives corrupted data on road hazards and vehicle position.

AV cyber-attacks are a known reality. These attacks demonstrate that attackers can take advantage of weaknesses in the network or sensor layers which could interfere with navigation or allow them to take control. If attacks were to occur in India this could result in vehicle malfunctioning to traffic disruption and exposure of data. These threats are practically possible and demand robust cyber security safeguards.

XII. LEGAL FRAMEWORK IN INDIA

Cyber security concerns are increased when AI, cloud connection and sensor driven communication systems are integrated into autonomous vehicles. This risk could endanger public infrastructure and safety of people. India lacks a separate legislation for AV cyber security existing framework under IT Act and DPDP do not directly address AV related operations through, statutory interpretation this paper substantiates that AV falls under computer and cyber offences. The DPDP Act ensures protection of personal data and mandates to give data breach report.

XIII. INFORMATION TECHNOLOGY ACT, 2000

a. Classification of Autonomous vehicle under IT Act 2000

Whether AV falls under computer?

Section 2(1)(i) of the Information Technology Act, 2000 defines a computer as any electronic, magnetic, or optical data processing device that performs logical, arithmetic, and memory functions through the manipulation of electronic or optical impulsesand includes all input, output, processing, storage, computer software or communication facilities which are connected or related to the computer in a computer system or computer network; An autonomous vehicle can very well fall within this definition as it is capable to perform logical, arithmetic and memory functions as stipulated under the definition. In response to real-time environmental conditions its onboard computer system performs logical functions by analyzing sensor inputs anddecidingappropriate driving actions, whether to brake, accelerate, or change lanes. It performs arithmetic functions through its LiDAR and RADAR systems, which send out laser or radiosignals andthat bounce back upon hitting an object or pedestrian, thereby enabling the calculation of their speed, distance, and direction.The autonomous vehicle carries out memory function by collecting,storing and retrieving vast amount of data generated during its operation. Data includes sensor data, telemetry data, user data and connectivity data. These data help in real time decision making, enhancing future navigation, adaptive learning and safety monitoring etc., The sensors serve as input devices, the control systems operate as output units, and the internal communication network integrates these components to ensure continuous data processing and communication. Hence, an autonomous vehicle embodies all the essential characteristics of a computer as envisaged under the IT Act and may rightly be construed as a computer system within its statutory meaning. Sensors, cameras, CAN networks, and ECUs in an autonomous vehicle be broughtunder the definition of a computer under the IT Act, as they operate in connection with the vehicle’s onboard computer system.

In Syed Asifuddin v. State of Andhra Pradesh (2005 Cri LJ 4314), the Andhra Pradesh High Court held that a digital handset qualifies as a “computer” under Section 2(1)(i) of the Information Technology Act,

2000, since it is an electronic, programmable device capable of processing, storing, and transmitting data by manipulating electronic impulses. This landmark judgment has broadened the statutory interpretation of "computer" to include digital handsets and other programmable communication devices, significantly extending the scope of India's cyber law framework.
By analogy, an autonomous vehicle similarly consists of programmable, electronic devices (ECUs, sensors, communication networks) that process, store, and transmit information to perceive the environment and control the vehicle. This judgment supports the interpretation that autonomous vehicles, as integrated electronic systems, clearly qualify within the statutory definition of a computer under the IT Act.

Whether it falls under computer Network?
An autonomous vehicle fits with definition of a "computer network" under Section 2(1)(j) of the Information Technology Act, 2000, becauseit interconnects multiple computer systems and communication devices such as sensors, ECUs, and camerasthat exchange data through Controller Area Network (CAN) or wireless communication links. These interconnected systems inside the vehicle, subsystems communicate constantly and exchange data about the its surroundings and speed to ensure safe navigation and decision making, whether or not the inter- connection is continuously maintained.
Externally, the vehicle connects via Vehicle- to-everything (V2X), towards other vehicles, and cloud platforms using wireless and satellite media. The conditions of Sec 2(1)(j) are met by these interconnected components by complying with both requirements,being interconnection through communication media and interaction between two or more computing or communication devices

Whether it falls under computer system?
An autonomous vehicle can very well be qualified as a computer system under Section 2(1)(l) of the IT Act, 2000, as it is a collection of devices including input and output support devices that perform logic, arithmetic, data storage and retrieval, and communication control functions. The vehicle's sensors, cameras, LiDAR, and radar collect input data from external environment, while the onboard computer and software process electronic instructions and stored data to make driving decisions which will be executed through output devices like actuators and control units.

Whether it falls under computer resources?
Under section 2(1)(k) the IT act defines "computer resource," means computer, computer system, computer network, data, computer data base or software; the entire AV ecosystem comprising hardware, software, and communication framework are encompassed by this broadened definition.

b) Cyber offences under IT Act
Section 43 of IT act can be effectively made applicable to punish a cyber-crime committed against an autonomous vehicle since, it can be legally be considered as "computer", "computer network", "computer system", and "computer resources" Hence any person causing damage to computer, computer system etc., is subject to civil liability under this section, includes payment of compensation. When it comes to AVs the following classifications explain how each subsection operates in context of Autonomous vehicles.
Section 43 lists out various offenses related to an unauthorized access and manipulation of self-driving vehicles. Key violations include:
a) gaining unauthorized access to internal systems such as CAN,
b) Downloading, copying, extracting data like GPS logs, user preference, driving history without consent
c) introducing malware or harmful codewhich could impair its driving logic or safety functions
d) damaging operational software or sensors
e) disrupting vehicle communication systems
f) denying legitimateusers access to vehicle controls through keyless entry,ECU lockout
g) aiding an offender by providing tools for hacking,
h) Charging services to another user's account,
i) destroying, deleting or altering information stored in an autonomous vehicle's onboard system.
j) tampering with source code or driving algorithms by altering or reverse engineering.
Section 43 of IT act, does not require the presence of mensrea to constitute an offence whereas section 66 of the act punishes the same offences when it is done dishonestly or fraudulently.

Sec 43A IT Act

This section provides compensation for data breaches, anybody corporate handles sensitive personal data in a computer resource owned, controlled or operated by it and maintain reasonable security practices and procedures. If body corporate fails to maintain or handle such data, results in negligence and causes loss to any person then such body corporate is liable to pay compensation to affected person.

Since autonomous vehicles rely on computers, sensors and network for data collection so these vehicles fall under computer resources under the Act. AV manufacturers and company must adhere to cyber security standards to prevent unauthorized access, data leaks. Negligence occurs when they fail to adopt necessary technical standards or update them. This may happen trough weak encryption, delayed software updates or poor access control. The company would be liable to pay compensation to affected individuals. The liability is not limited to car manufacturers alone but it extends to software developers and cloud service providers but it requires a continue due diligence to maintain cyber resilience and data security throughout the AVs life cycle.

Reasonable security practices and procedures

It defines technical and organizational measures to safeguard data from unauthorized access, modification or disclosure.These Security practices can be established through contractual agreements such as ISO/SAE 21434 for vehicle cyber security or may be mandated by law including IT (Reasonable security practices and procedure and sensitive personal data or information) Rules 2011 or DPDP Act 2023.The term "reasonable security practices and procedures" used under Section 43A of the IT Act, 2000 remains undefined, making it ambiguous and open to interpretation. While the 2011 Rules attempt to explain it by referring to ISO/IEC 27001 standards and documented security policies, the term "reasonable" is still too general and fails to reflect the unique cybersecurity needs of different industries, especially the autonomous vehicle (AV) sector. Given the complex software architecture and data-driven functioning of AVs, "reasonable security practices" should explicitly include additional safeguards such as secure software design, supply chain integrity assurance, protection for over-the-air (OTA) updates, and regular vulnerability assessments. To ensure legal and technical adequacy, the 2011 Rules should be amended to incorporate automotive-specific cybersecurity standards like ISO/SAE 21434 (Road Vehicles CyberSecurity Engineering) and the UNECE WP.29 Regulation on Cybersecurity and Software Updates, which set globally recognized benchmarks for securing vehicle data, communication networks, and software systems. This amendment would provide much-needed clarity and industry-specific precision to the otherwise vague concept of "reasonable security practices."

In DhuleVikasSahakari Bank Ltd. v. Axis Bank Ltd. (2025), Axis bank was held strictly liable for not maintaining reasonable security practices. Axis bank fails to enforce cyber security standards, so this results in substantial financial loss. With respect to autonomous vehicle AV manufacturers, service providers would be liable under section 43A for failure to implement cyber security protocols. Victims can claim compensation if an AV system is compromised as a result of inadequate security measures leading to unauthorized data accessor remote vehicle control.

Section 66C

Whoever fraudulently uses another person's electronic signature, password or unique identification shall be punishable for identity theft. With respect to AV vehicle E-signatures involves digital certificates, cryptographic keys, biometric identifiers that verify identities of vehicles, users or system node. AV utilize these digital identities for secure communication and software updates. If hacker clones an AV'S digital certificate and steals a manufacturer's signing key or forges an owner's digital key such actions constitute fraudulent use of another's electronic signature amounts to identity theft and punishable under section 66C IT Act.

Section 66F

Section 66F IT Act defines cyber terrorism, which refers to unauthorized digital acts aimed at threatening India's security and integrity or sovereignty of India. It encompasses activities death, injury or disruption of essential services. It also includes serious attacks on critical information infrastructure under this Act. AV depends on interlinked computer system, cloud network and V2V Communication which are vulnerable to large scale cyber-attacks. Such an attack could hijack the AV fleet, disrupt traffic or manipulate

navigation resulting in a mass collision that would amount to cyber terrorism.

c) Critical Information infrastructure and Incident reporting Framework

Section 70A

Section 70A of the Information Technology Act, empowers the Central Government to appoint a national nodal agency for protection of CriticalInformation Infrastructure (CII). As defined under section 70 "Critical Information Infrastructure" means the computer resource, the incapacitation or destruction of which, shall have debilitating impact on national security, economy, public health or safety. The National Critical Information Infrastructure Protection Centre (NCIIPC) is designated as such nodal agency appointed by central government, which recognizes six vital sectors required to be protected includes energy, banking and finance, telecom, transport, government, and strategic and public enterprises. Transportationbeing one of these sectors, an autonomous vehicle be effectively protected under the NCIIPC, provided when they are deployed as a part of public transport systems such as robotaxi similar to that of Waymo in US or smart bus fleets. It is not the vehicle as an isolated unit be protected the cloud computingplatforms, communication network, and data infrastructure that support autonomous vehicle operations would be secured under NCIIPC.

If protected by NCIIPC, an autonomous vehicle would be required to ensurestrict cybersecurity measures and regular vulnerability assessments. This improves the overall efficiency of an autonomous vehicle and thereby making it less prone to vulnerabilities and cyber-attacks.

Section 70B

The Indian Computer Emergency Response Team (CERT-In) is established as the national agency under section 70B. Its functions include collecting and analyzing information on cyber threats, forecast and alerts of cyber security incidents, emergency measures for handling cyber security incidents, coordinating emergency responses, and providing security guidelines, advisories, vulnerability notes and white paper relating to information security practices, procedures, prevention, response and reporting of cyber incidents This provision is broad in nature to extend CERT-In to function on the area of cybersecurity of an autonomous vehicle including detecting cyber-attacks on vehicle's network,issuing advisories to manufacturers, and coordinating responses with transport and law-enforcement authorities.

Autonomous vehicles collect sensitive personal data, which is regulated under the DPDP Act, 2023 to ensure lawful and responsible processing. Because this data is generated and stored within an onboard computer system, it becomes exposed to risks such as hacking, spoofing, and unauthorised access. These system-level cyber threats are addressed by the IT Act, 2000, forming a complementary framework between data protection and cybersecurity.

The Indian Computer Emergency Response Team (CERT-In) is established as the national agency under section 70B. Its functions include collecting and analyzing information on cyber threats, forecast and alerts of cyber security incidents, emergency measures for handling cyber security incidents, coordinating emergency responses, and providing security guidelines, advisories, vulnerability notes and white paper relating to information security practices, procedures, prevention, response and reporting of cyber incidents. The practical scope of this section remains narrow for autonomous-vehicle systems, because it is designed around general IT environments rather than safety-critical vehicular networks. Autonomous vehicles rely on specialized communication protocols, real-time data flows and complex in-vehicle architectures that demand continuous sector-specific expertise. CERT-In operates under the administrative control of the Department of Electronics and Information Technology. The Information Technology (CERT-In and Manner of Performing Functions and Duties) Rules, 2013, empower CERT-In with functions including mandatory incident reporting (Rule 12) and powers to monitor and collect traffic data under Section 69B (Rule 14). In 2022, the government introduced additional directions mandating incident reporting within six hours, retention of logs for 180 days within India, and requirements for cloud services, data centers, and VPN providers to maintain customer details, thereby strengthening national cybersecurity.

XIV. DIGITAL PERSONAL DATA PROTECTION ACT, 2023

The object of DPDP Act 2023 is to safeguard the personal data of individuals while making sure that data processing by organization is legal and accountable. Its main goal is to strike a balance between a person's right to privacy and the legitimate use of data for innovation, governance and corporate operations. This Act applies only to digital personal data, where non personal and non-digital data are not governed under this Act.

Autonomous vehicle relies on continuous data like processing, collecting personal information such as location, driver identity, voice data and behavioral patterns. This makes them vulnerable to cyberattacks and data breaches. DPDP Act which complements Information technology Act 2000, emphasizes the collection, storage, security and protection of personal data before and after such incidents.

Section 2 This section defines key terms included in the act to ensure consistent interpretation. The key terms are explained as follows.

i) Section 2(i) defines Data fiduciary," means any person who determines the purpose and means of processing of personal data, with manufacturers and software developers as fiduciaries in autonomous vehicles (AVs).

ii) Section 2(j) defines Data principal refers to the individual to whomthe personal data relates, with respect to AVs passenger or driver is regarded as such.

iii) Section 2(t) defines Personal data means any data identifies an individual that includes navigation data, drivers' identityand passengers' identity in case of robotaxi, voice commands, and location data, facial recognition data, app identifiers, in-camera footage for AVs.

iv) Section 2(u) defines Personal data breach means any unauthorized processing of personal data that compromise the confidentiality, integrity, or availability, exemplified by hacking incidents that expose passengers' travel details or biometric data in AVs.

Consent protection and data protection board

Consent and lawful purpose

Data fiduciary can process a data principal's personal data and it should be used only for lawful purpose where data principal has given consent which is mentioned under Section 4DPDP Act. Section 6 says that such consent given by data principal should be free, informed, specified and unambiguous consent. AV manufacturers and service providers are required to obtain explicit consent from users (data principals) before collecting data such as location, biometrics, in cabin recordings and driving pattern. Such consent obtained must be clear and not embedded in terms and condition should provide clear options like app based or dashboard notifications.

Illustration –If AV manufacturer wants to collect camera footage or location details for improving driving algorithm it must give a clear message on the app to have users' approval.

Consent process for AVs is mentioned under DPDP Rules 2025.

Rule 3- AV system to present clear data use notice before requesting user's consent.

Rule 4- OEMs or AV service providers keep consent records and offer users the ability to review or withdraw their consent at any time.

Data protection Board of India (DPBI)

Section 18 DPDP Act establishes the data protection board of India as an independent body under the central government and ensure compliance with DPDP Act. This board addresses complaints or breaches concerning personal data. In case of data breach must report to DPBI.

Powers and functions of Board – Sec.27

- Board has authority to investigate data breaches reported by data fiduciaries or individuals
- It has authority to impose penalties for violations
- Board can summon information, examine witnesses and conduct hearings like civil court.
- It handles grievances and complaints from data principals
- Advice the government on data protection

In the AV ecosystem, OEMs or service providers facing a cyber-attack or data breach may submit a voluntary undertaking under Section 27 to enhance cyber security measures and improve data handling thereby avoiding heavier penalties and showing good faith compliance.

Rule 7 of DPDP Rules, 2025

Data protection board of India mandates that all personal data breaches be reported within 72hours by data fiduciaries. Data fiduciaries must inform both the

affected individuals and board. Duty of board to monitor significant data security incidents, investigating noncompliance and directing appropriate remedial actions.

In autonomous vehicle, Rule 7 mandates that AV manufacturers and service providers should quickly report about the cyber-attacks or data leaks to data protection board of India (DPBI) for regulatory oversight and user protection.

XV. INDIAN STANDARDS FOR AUTONOMOUS VEHICLE

Automotive Research Association of India (ARAI) is India's leading automotive testing, research and certification organization operating under ministry of heavy Industries. ARAI is central to devising and implementing vehicle testing and certification protocols. The ministry of road transport and highways (MoRTH) oversees automotive standards under the central motor vehicle Rules (CMVR), collaborates with ARAI to offer type approval, safety testing and compliance certification. ARAI has created the Draft AIS -189 titled under "Approval of Vehicles with regards to Cyber Security and Cyber Security Management System (CSMS)" which introduces a structured cyber security framework for vehicles equipped with Level -3 automation and above.This standard specifies standards for supply chain security, software update processes, risk assessment and cyber security management system.Currently AIS 189 is a draft form and it is not mandatory in nature. As a result, CMVR remains a regulatory bottleneck. In order to provide legally robust, technologically secure and uniform framework for AV cars in India, MoRTH and ARAI must formally enforce AIS 189. Automakers would be required to incorporate supply chain cyber security controls and structured risk assessments as part of the AIS 189. Mandatory implementation and certification process would improve accountability and public trust.Implementing AIS -189 under the central motor rules would bridge the existing regulatory gap, shift India's focus from physical safety to integrated cyber physical resilience and ensure safe, reliable and innovative introduction of autonomous vehicle on Indian roads.

XVI. CHALLENGES FOR ADOPTING AUTONOMOUS VEHICLE IN INDIA

- There is no dedicated legislation for AV liability or data protection in India
- Data privacy and cyber security risk arises due to inadequate protection laws
- Poor road infrastructure and unpredictable traffic make difficult for implementing AV Vehicles in India
- AIS -189 standards in India have not been fully enforced, it limits the regulatory certainty.
- Lack of statutory enforcement under central motor vehicle rules hinders standardized testing and cyber security compliance.
- AV flexibility is hampered by unpredictable pedestrian and driver behavior.
- There are no explicit guidelines about who is liable for accident whether AV manufacturer or service provider
- Lack of binding implementation in India is limiting advancements in AV innovation and public deployment.
- Insufficiently skilled engineers, technicians and legislators to integrate AV.

XVII. MODEL FRAMEWORKS OF OTHER COUNTRIES

1. US

There is no unified national law governing autonomous vehicle in US instead each state establishes its own regulation for AV testing, deployment and operational requirements. Even though there is no unified legislation for AV but there are federal vehicle safety requirements and testing procedures that are applicable in every State. These norms offer a baseline of consistency.

Regulatory Authorities

NHTSA

In an effort to foster domestic innovation, US transport secretary Sean P. Duffy unveiled the new national highway traffic safety Administration 2025 for AV framework aimed at promoting domestic innovation. This framework emphasizes three principles

1. Ensuring the safety of AV operations.
2. Reducing unnecessary regulatory barriers

3. Support the commercial deployment of AVs to improve safety and mobility

Initial action includes the issuance of Third amended standing order 2021and the expansion of automated vehicle exemption program to include domestically produced vehicle.There are 2 new policy development 1.NHTSA issued a third amended standing order 2020 and came into force on June 2025, governs incident reporting for vehicles with Automated Driving systems (ADS) and level 2 or higher Advanced driver assistance systems (ADAS). The amendment streamlines the reporting process by extending the incident report submission timeline within 5 calendar days after notice of the incident.

2.NHTSA has brought Automated vehicle exemption program (AVEP) to include vehicles manufactured in US. Previously NHTSA had authority to exempt imported vehicles that did not adhere to specific Federal motor vehicle safety standards (FMVSS) under 49 C.F.R. Part 591 as long as they were brought for demonstration, testing or research purpose only and not for commercial sale. Similar exemptions are now available to American manufacturers working on AV development and testing. This facilitates the legal testing of AVs, which speeds up innovation.

Black box (EDR)

Event data recorder helps investigators assess the functionality of safety equipment by capturing vital safety information during AV accidents it is known as black box. This information informs future designs and regulations and supports current advancements in vehicle safety. Investigators can evaluate the effectiveness of certain safety devices both before and during an accident with the use of this information. Similar to an airplane's flight data recorder (FDR) every AV should have an EDR to track and record vehicle performance. This technology helps to identify whether crashes are caused by mechanical failure or human mistake. Manufacturers will be held liable by the use of EDR data. In 2006 NHTSA mandates automakers to collect specific data via EDR such as vehicle speed, crash forces at impact, airbag deployment, brake application before a crash. Honda is additionally gathering EDR data voluntarily to assess the functionality of its advanced driver assistance systems.

Case studies in US

1. Jeep Cherokee Hack case (2015)

Researchers Charlie miller and Chris Valasek remotely hacked a jeep vehicle in 2015, through Uconnect cellular interface, gaining access to the CAN bus and managing vital systems like steering and brakes. It showed the possibility for manipulation of internet connected car systems. This illustrates how insufficient network segmentation could compromise safety critical system through infotainment and telematics access. It serves as a warning for AVs that depend heavily on sensors and networked software, emphasizing the necessity for robust cyber security practices to prevent harm through network vulnerabilities.

2. Cruise AV pedestrian case (2023)

Cruise autonomous vehicle from General Motors struck and dragged a pedestrian after she was initially hit by a human driver car. According to investigations, AV failed to stop the hit and instead pulled the victim forward, demonstrating an inappropriate response. Because of safety concerns and insufficient incidence data disclosure, the California DMV suspended cruise driverless testing permits as a result of this occurrence. It emphasis the need for better cyber security and safety procedures and shows the accountability gap in AV operations.

2. EU

The regulatory framework of EU for anautonomous vehicle has developed gradually,that indicates its commitment to strike a balance between innovation with safety and accountability.

Vehicle type approval Regulation (EU) 2018/858

This governs the overall approving of new vehicle types across all member states of EU, ensuring uniform safety and security standards and serve as the legal basis for subsequent regulation and approval procedures specific to autonomous vehicles.

Guidelines on exemption procedure for the EU approval of Automated vehicle, 2019

The European commission introduced an exemption procedure that allows vehicle type approval by national ad hoc safety assessment to bridge the gap left by Regulation (EU) 2018/858, until a detailed harmonized regulation was adopted. As per this procedure the manufacture must define what is the vehicle's operational domain(OD) and where ,when

the automated driving system is designed to operate, they must demonstrate that it is safe by design, compliance with traffic rules, interacting predictably with other road users, mandates every vehicle must include a Black box (event data recorder) to record operational data to ensure accountability, and comply with EU data protection and cyber security standards. The Approval is granted only after the compliance with standards.

General safety Regulation (EU) 2019/2144

To strengthen the technical provisions discussed in exemption process guidelines, it sets out specific requirements related to a fully autonomous vehicle under article 11. It mandates that such vehicle shall comply with the technical specification for systems that replace the complete control of the driver, provide the vehicle with real time information of its surroundings, and include event data recorder and data sharing mechanisms for coordinated driving. This regulation in order to promote consistent process and technical requirements obligates European commission to adopt acts for purpose of implementation.

Implementing Regulation (EU) 2022/1426

This regulation is introduced for the purpose of issuing guidelines for implementation of Regulation (EU) 2019/2144.

The purpose of this regulation is to establish guidelines for the implementation of Regulation (EU) 2019/2144 for the type-approval of automated driving systems (ADS) of AVs.

It establishes the technical and procedural framework EU type approval to fully autonomous vehicle with ADS. It specifies requirements for functional and operational safety, cybersecurity compliance, software updates and data recording in compliance with UN regulation.Requires manufacturers to submit documentation proving that ADS is free from unreasonable safety risks to occupants and other road users.

The ADS is required to perform anticipatory and cooperative behavior in traffic, avoiding collisions by adapting speed, maintaining safe distances, and executing emergency maneuvers while giving priority to human life and safety of all road users in various nominal and critical traffic scenarios. In addition to the regulatory framework established by this regulation, European Transport safety council (ETSC) plays a vital role in advocating for implementing stringent safety standards in deployment of AV. It articulates that the AV should undergo rigorous real world driving tests to operate in a complex traffic environment and be subjected to continuous safety evaluations to align with the prescribed standards. The ETSC recognise the necessity for harmonized testing protocols to prioritize public safety alongside technological innovations.

In contrast, the Indian framework under the IT Act, CERT-In Directions 2022, and the draft AIS-189 provides only a foundational structure. These instruments set general cyber-incident duties and a basic Cyber Security Management System but do not yet provide EU-level components such as ADS-specific type-approval procedures, mandatory ODD validation, black-box data-recording obligations, real-world test requirements, coordinated data-sharing mechanisms, or integrated safety and cyber-security assessments. This regulatory gap shows that while India has initiated essential groundwork, several advanced elements present in the EU regime are not yet incorporated in the Indian legal and technical framework.

Regulation of personal data in EU- GDPR

The DPDP Act already covers most GDPR principles such as lawful processing, purpose limitation, accuracy, storage limits, security safeguards and the right to withdraw consent. For autonomous vehicles these protections are adequate for basic data governance. The one element of GDPR that remains specifically relevant and not expressly reflected in the DPDP Act is granular consent under Recital 32. Autonomous vehicles collect different categories of data at the same time, so separate consent for each category becomes important for clarity and control.

XVIIICONCLUSION

This paper demonstrates that, since an AV can be interpreted as a computer or computer system under the IT Act, 2000, the existing legislative framework with minor targeted amendments, iswell equipped to address the cybersecurity and data protection issues. The DPDP Act, 2023, along with its rules, governs the personal data collected by AV technologies. Considering this basis, the study concludes that India

doesn't need new AV specific-legislation; rather, it requires a targeted regulatory measure, effective implementation of standards provided by AIS-189 which, currently remain non-mandatory and lacking binding certification timelines and safety disclosure requirements.

XIX. SUGGESTIONS

1. Mandatory Event data recorders (EDR)- Install black box style EDRs in all autonomous cars to record crash, capture and cyber event data for regulatory and forensic examination.This black box tracks and record vehicle performance before and after the incident.
2. Joint AV cyber security sandboxes- It creates multi agency regulatory (CERT, DPB,MoRTH) to jointly test data sharing protocols, governance models and frameworks for responding to cyber incidents.
3. AV safety and regulator – Establish an independent body (similar to US NHTSA) to supervise AV Testing, deployment, cyber security guidelines and recall procedures in collaboration with CERT and DPB.
4. Amend Section 70B IT Act – Establish a dedicated specialized sub-division, within CERT-In specific for AV systems
5. Granular consent under DPDP Act – Need Granular consent to ensure transparency and lower security risk in AV ecosystem by making sure data principals are aware of the precise data categories which is shared with data fiduciaries.
6. Reasonable Security under Section 43A- The definition of reasonable security under Section 43A vague. It should specifically cover protections to the automotive sector like supply chain assurance, secure OTA upgrades and frequent vulnerability testing.
7. Mandatory certification and incident reporting – Require ARAI/BIS certification for AV cyber security prior to deployment and there should be mandatory disclosure of cyber incidents of AV vehicles and third-party security audits.
8. Compliance with Global standards- Align cyber security certification and testing for Indian AV with ISO/SAE 21434 and UNECE WP.29.
9. Mandate AIS 189- In accordance with central motor vehicle rules, notify AIS-189 to require adherence to cyber security management systems.
10. Implement Third party testing standards and audits- In order to guarantee public safety and security, it requires Third party testing and audits by ARAI agencies.

REFERENCES

[1] https://iipseries.org/assets/docupload/rsl20245180E2B3C382493.pdf
[2] https://www.livelaw.in/lawschoolcolumn/liability-for-self-driving-vehicles-automated-cars-driverless-technology-212778
[3] https://jolt.law.harvard.edu/assets/articlePDFs/v32/32HarvJLTech299.pdf#:~:text=proprietary%20software%20owned%20by%20the%20vehicle%20manufacturer
[4] https://netrality.com/blog/the-role-of-data-center-network-connectivity-in-powering-the-future-of-autonomous-vehicles/
[5] https://en.wikipedia.org/wiki/Self-driving_car_liability
[6] https://www.researchgate.net/publication/362947016_The_Liability_Limits_of_Self-Driving_Cars
[7] https://blog.kambria.io/the-history-and-evolution-of-self-driving-cars/
[8] https://www.researchgate.net/publication/362947016_The_Liability_Limits_of_Self-Driving_Cars
[9] https://ec.europa.eu/docsroom/documents/34802/attachments/1/translations/en/renditions/native
[10] https://www.sei.cmu.edu/blog/vehicle-cybersecurity-the-jeep-hack-and-beyond/.