International Journal of Scientific Research & Engineering Trends
Volume 12, Issue 2, Mar-Apr-2026, ISSN (Online): 2395-566X

Data Protection and Cybersecurity Issues in Autonomous Vehicles Under Indian Law

Nv Subhasri, Madhunisha. A, Shruthi. T

Department of LAW

Abstract: This dissertation examines the growing intersection of law, technology, and regulation in the context of autonomous vehicles (AVs) in India, with particular emphasis on issues of privacy, data protection, and cybersecurity. It analyzes existing Indian legal frameworks, such as the Information Technology Act and the proposed Personal Data Protection Bill, to assess whether they are equipped to handle the unique challenges posed by AV technology. The study also compares India's approach with international standards, including the GDPR and regulatory models followed in countries like the United States and China. Through this comparative perspective, the research highlights existing gaps and suggests areas where India can strengthen its legal and regulatory response.

Keywords: Autonomous Vehicle Regulation, Privacy, Data Protection, Cybersecurity

I. INTRODUCTION

In today's rapidly evolving technological world, autonomous vehicles (AVs) are emerging as one of the most exciting and transformative innovations. These self-driving cars, capable of operating without human control, have the potential to completely change the way we travel by making transportation more efficient, safer, and environmentally friendly. However, as this technology slowly moves from theory to reality—especially in a country like India—it also brings along several legal and ethical challenges, particularly related to privacy and data protection.

The introduction of AVs in India is not just about technological advancement; it also tests how well our legal system can adapt to protect individual rights in a digital era. The functioning of these vehicles depends heavily on advanced technologies such as sensors, cameras, and data-processing systems. While these features enable smooth and intelligent operation, they also continuously collect large amounts of data. This may include personal information such as travel habits, daily routines, and even in-vehicle interactions. If this data is not properly secured or is misused, it could lead to serious privacy concerns.

This topic becomes even more important in light of India's recent developments in privacy law. A key milestone was the Supreme Court's judgment in Justice K.S. Puttaswamy (Retd.) vs. Union of India, which recognized the right to privacy as a fundamental right. Despite such progress, discussions around autonomous vehicles and their impact on data privacy are still at an early stage in India. Through this dissertation, an attempt is made to address this gap by examining the privacy and data protection issues associated with AVs, evaluating whether existing laws are sufficient, and suggesting possible legal reforms to better regulate this emerging technology.

Background Information

India, known for its rich cultural diversity and long history, is now at an important stage where it is beginning to adopt advanced technologies like autonomous vehicles (AVs). What was once seen only in science fiction has now become a reality, with self-driving cars slowly transforming transportation systems across the world. The development of AV technology can be traced back to the 1980s, with early initiatives such as the EUREKA Prometheus Project, which laid the foundation for modern autonomous systems. Later, in the early 2000s, rapid improvements in areas like machine learning, sensors, and computing power helped this technology grow significantly.

A major turning point came in 2009 when Google launched its self-driving car project, showing the world the real potential of autonomous vehicles. In India, interest in AVs has been steadily increasing, mainly due to the need to solve major issues like traffic congestion, road accidents, and pollution in cities. Many believe that AVs could offer effective solutions to these problems by making transportation more efficient and safer.

In response to this growing interest, Indian automobile and technology companies have started investing in research and development related to AVs. Several pilot projects and collaborations are being carried out to adapt this technology to Indian road conditions, which are quite different from those in other countries. Partnerships between institutions like the Indian Institutes of Technology (IITs) and private companies are playing an important role in this development. For example, Mahindra & Mahindra, in collaboration with IIT Bombay, has been working on developing autonomous electric vehicles suited for Indian environments. Government initiatives like the Smart Cities Mission are also indirectly supporting the integration of AVs into urban transport systems.

However, along with these technological advancements, there are also serious concerns, especially regarding privacy and data protection. Autonomous vehicles rely on various technologies such as cameras, GPS, and LiDAR sensors to function, which means they constantly collect large amounts of data about their surroundings and users. This raises important questions about how this data is stored, used, and protected. There have already been global instances of data breaches and hacking incidents involving vehicle systems, highlighting the risks involved.
India has taken some steps towards strengthening data protection through laws like the Information Technology Act, 2000, and the Digital Personal Data Protection (DPDP) Act. Additionally, the Supreme Court's judgment in Justice K.S. Puttaswamy (Retd.) vs. Union of India (2017) recognized privacy as a fundamental right, which has strengthened the legal position on data protection.

Despite these developments, there are still no specific laws that directly address the challenges posed by autonomous vehicles. Existing regulations do not fully cover issues such as user consent, data sharing, and cross-border data transfers in the context of AVs. This creates important gaps in the legal system, making it necessary to update and strengthen current laws to ensure that technological progress does not come at the cost of individual privacy.

Overall, the development of autonomous vehicles in India presents both opportunities and challenges. Understanding this balance is important, and this dissertation aims to explore these issues in detail by examining the current legal framework and suggesting improvements to better regulate this emerging field.

Dissertation Structure Overview
Introduction The dissertation begins with an introduction to autonomous vehicles (AVs) and how they connect with issues of privacy and data protection in India. This chapter sets the foundation by explaining the importance of AV technology in today's world and the legal and ethical concerns that come along with it. It also outlines the main aim of the study and presents the research questions, focusing on whether the current Indian legal system is prepared to deal with privacy challenges created by AVs.

Literature Review This chapter looks at existing studies, research papers, and legal discussions related to autonomous vehicles, privacy, and data protection. It brings together information from different sources like academic articles, legal frameworks, and technological studies to build a strong base for the research. It also explores how other countries have dealt with similar issues and examines global developments in AV technology and privacy concerns. This helps in understanding how these ideas can be applied to the Indian context.

The Technology of Autonomous Vehicles In this section, the focus is on understanding how autonomous vehicles actually work. It explains the role of technologies such as sensors, GPS, LiDAR, and machine learning in enabling self-driving systems. Since these technologies rely heavily on data collection and processing, this chapter also highlights how privacy concerns arise in real-life situations and what kind of technological solutions can help reduce these risks.

Legal Framework and Case Law This chapter forms a key part of the dissertation by examining the existing Indian laws related to privacy and data protection. It discusses important court judgments, including decisions by the

Supreme Court, that have shaped the right to privacy in India. It also compares Indian laws with international standards like the GDPR and legal approaches followed in countries such as the United States. This comparison helps in identifying areas where Indian laws may need improvement.

Analysis and Findings Here, the study brings together all the information collected from earlier chapters. It analyzes legal provisions, case laws, and technological aspects to answer the research questions. This section highlights important patterns, identifies gaps in the current system, and evaluates whether existing laws are sufficient to deal with the challenges posed by autonomous vehicles.

Recommendations and Conclusion The final chapter provides suggestions based on the findings of the research. It recommends possible changes in laws and policies to improve data protection and privacy in the context of AVs. The conclusion also reflects on the overall importance of the study and how it can help policymakers, legal professionals, and technology developers create a safer and more privacy-focused environment for the use of autonomous vehicles in India.

Methodology Overview This dissertation follows a multidisciplinary approach by combining legal analysis, technological understanding, and case study evaluation. This method helps in giving a well-rounded view of the topic and ensures that the issue is studied from different perspectives.

Importance of the Study Lastly, this section highlights why the study is important. By connecting law, technology, and policy, the research aims to contribute to ongoing discussions about privacy and data protection in India. It also seeks to support the development of stronger legal frameworks that can effectively deal with emerging technologies like autonomous vehicles while protecting individual rights.

II. THE TECHNOLOGY OF AUTONOMOUS VEHICLES

Technical Overview of Autonomous Vehicles

Autonomous vehicles (AVs) represent a major advancement in modern automobile technology, marking a shift towards systems that can function without direct human control. These vehicles, once imagined only in science fiction, are now becoming a reality due to rapid developments in both hardware and software technologies. At their core, AVs are designed to replicate and even enhance the abilities of a human driver by integrating multiple complex systems that work together seamlessly.

The technology behind AVs focuses on combining sensors, computing systems, and intelligent algorithms to perform tasks such as navigation, obstacle detection, and decision-making. This integration allows the vehicle to operate independently while adapting to real-world driving conditions.

Sensors and Perception Systems

A key component of autonomous vehicles is their perception system, which is made up of various sensors and cameras that continuously gather data about the surrounding environment. This data is essential for ensuring safe and efficient vehicle operation

One of the most important technologies used is LiDAR (Light Detection and Ranging), which creates detailed 3D maps by sending out laser beams and measuring how they reflect off objects. This helps the vehicle understand its surroundings with high accuracy.

Radar sensors are also used to measure the speed and distance of nearby objects. These are especially useful in situations where visibility is poor, such as during heavy rain or fog.

Ultrasonic sensors play a role in detecting objects at close range, making them useful for low-speed movements like parking.

In addition, optical cameras act as the “eyes” of the vehicle. They capture visual data, enabling the system to recognize road signs, traffic lights, pedestrians, and other vehicles. All this information is sent to the vehicle’s processing system for further analysis.

Computational Systems and Software

At the centre of an AV is its computational system, which processes the vast amount of data collected by sensors. This system relies on advanced software and machine learning algorithms to interpret complex driving situations and make informed decisions.

These algorithms are trained using large datasets that include various driving scenarios, allowing the vehicle to learn patterns and improve over time. The ability to process data in real time is critical, as the vehicle must respond instantly to changes in its environment.

The software structure usually consists of multiple layers, each responsible for analyzing different aspects of the driving environment. Together, these layers ensure that the vehicle can make safe and accurate decisions.

Connectivity and Integration

Modern autonomous vehicles are designed to communicate with their surroundings using technologies like vehicle-to-everything (V2X). This allows vehicles to share information with other vehicles, infrastructure, and traffic systems.

For example, if one vehicle detects an obstacle or suddenly brakes, it can instantly communicate this information to nearby vehicles. This improves safety and helps in better traffic management.

Such integration also includes communication with traffic signals and road systems, which is an important step toward developing smart cities where transportation systems are interconnected and efficient.

Navigation and Control Systems

Navigation systems in AVs combine GPS data with sensor inputs to create accurate and flexible route plans. These systems are continuously updated based on real-time conditions such as traffic or roadblocks.

Control systems are responsible for executing driving actions like steering, braking, and acceleration. They ensure that the vehicle follows traffic rules, maintains safe distances, and reacts appropriately to road conditions.

Data Collection and Processing

Data Collection in Autonomous Vehicles

Autonomous vehicles depend heavily on data collection for their operation. They gather different types of information, including geographic location through GPS, visual data from cameras, and distance measurements using radar and LiDAR.

They also collect data related to their own functioning, such as speed and braking patterns, as well as user-related data like preferences and behaviour. While this enhances performance and user experience, it also raises concerns about privacy.

Data Processing in Autonomous Vehicles

The collected data is processed in two main ways.

Real-time processing allows the vehicle to make immediate decisions, such as avoiding obstacles or adjusting speed. This requires powerful computing systems capable of handling data instantly.

Long-term processing involves analysing stored data to improve system performance over time. This helps in refining algorithms and updating navigation systems.

Data Integration and Synthesis

Data from multiple sources is combined to create a complete understanding of the vehicle's environment. This integration helps improve decision-making by providing more accurate and comprehensive information.

However, it also results in detailed records of vehicle movements and user behaviour, which can raise serious privacy concerns if not properly managed.

Privacy and Security Concerns

The extensive data collection by AVs leads to important privacy and security challenges. Continuous tracking can reveal sensitive personal information, while interconnected systems increase the risk of cyberattacks.

Without proper safeguards, this data could be misused or accessed by unauthorized parties, making strong legal and technical protections essential.

Potential Privacy and Security Issues

Privacy Concerns

Autonomous vehicles collect large amounts of personal data, which can lead to several issues. Continuous GPS

tracking can reveal a person's daily routines and locations. Cameras may capture images of individuals without their consent.

Additionally, data on user behaviour and preferences can be used to create detailed profiles, which may be misused for commercial or other purposes.

Security Vulnerabilities

AV systems are vulnerable to cyber threats due to their reliance on connectivity. Hackers may attempt to access vehicle systems, leading to data breaches or even control over the vehicle.

Communication systems can also be intercepted, potentially causing incorrect responses or accidents. Software vulnerabilities further increase these risks.

Mitigating Risks

To address these challenges, several measures can be implemented. Encryption can protect data from unauthorized access, while data minimization can reduce privacy risks.

Regular software updates are essential to fix vulnerabilities, and strong legal frameworks are needed to regulate data use and ensure accountability.

III. LEGAL FRAMEWORK AND CASE LAW

Analysis of Indian Case Law on Privacy and Data Protection in the Context of Autonomous Vehicles

The legal framework in India relating to privacy and data protection has evolved significantly over time, especially with the development of constitutional jurisprudence through landmark Supreme Court judgments. These judicial decisions play a crucial role in shaping how emerging technologies like autonomous vehicles (AVs) are regulated, particularly since such technologies involve large-scale data collection and processing.

One of the most important cases in this context is Justice K.S. Puttaswamy (Retd.) vs. Union of India (2017), where the Supreme Court recognized the right to privacy as a fundamental right under Article 21 of the Constitution. This judgment has far-reaching implications for AVs, as it establishes that any technology handling personal data must ensure that individual privacy is protected. It emphasizes the need for clear legal safeguards when dealing with personal information, especially in systems that continuously collect and process data.

Another significant case is Shreya Singhal vs. Union of India (2015), where the Court struck down Section 66A of the Information Technology Act for being unconstitutional. This judgment highlights the importance of preventing excessive legal control over digital spaces, ensuring that laws do not unnecessarily restrict individual freedoms. In the context of AVs, it suggests that regulations must strike a balance between technological innovation and the protection of fundamental rights.

The case of Public Concern for Governance Trust vs. Union of India further addressed issues related to surveillance and data collection. The principles emerging from this case indicate that any form of surveillance must be legally justified and proportionate. This is particularly relevant for AVs, as their operation involves constant monitoring of surroundings and individuals.

Earlier cases such as Kharak Singh vs. State of Uttar Pradesh (1963) and District Registrar vs. Canara Bank (2005) also contribute to the legal understanding of privacy. These cases reinforce the idea that individuals have a right to protect their personal information and should not be subjected to unnecessary intrusion.

Application to Autonomous Vehicles

Based on these judicial precedents, certain key principles can be applied to autonomous vehicle regulation in India. First, there is a clear need for a strong data protection framework that governs how personal data is collected, stored, and used.

Second, consent plays a vital role. Users must be informed about data collection practices and should have the ability to control how their data is used.

Third, surveillance through AV technologies must be limited and legally justified to avoid unnecessary intrusion into personal lives.

Finally, transparency and accountability must be ensured so that individuals are aware of how their data is handled and can seek remedies in case of misuse.

Application of Existing Indian Laws to Autonomous Vehicles

The current legal system in India provides some foundation for regulating AVs, although it is not specifically designed for such advanced technologies.

The Information Technology Act, 2000 plays an important role in governing data protection and cybersecurity. Provisions like Section 43A require organizations to maintain reasonable security practices when handling sensitive data, while Section 72A penalizes unauthorized disclosure of information. These provisions can be applied to AVs, but they do not fully address the complexities of continuous data collection and real-time processing.

The Motor Vehicles Act, 1988 (as amended in 2019) primarily deals with traditional vehicles but includes provisions that could potentially be extended to AVs. It addresses issues like vehicle safety, certification, and liability, which are relevant for autonomous systems. However, it does not clearly define concepts such as who is responsible when an AV is involved in an accident.

The Digital Personal Data Protection (DPDP) Act represents a significant step forward in data protection law in India. It emphasizes principles such as consent, data minimization, and user rights. While these principles are relevant to AVs, the law does not specifically address how they apply to technologies that rely on constant data collection.

Comparative Analysis with International Law

Looking at international frameworks provides useful insights for India.

The European Union's GDPR is one of the most comprehensive data protection laws in the world. It focuses on user consent, data minimization, and strong privacy protections. Applying similar principles to AVs in India could strengthen data protection standards.

The United States follows a decentralized approach, where different states have their own regulations. This allows flexibility and adaptation to local conditions, which could be useful in a diverse country like India.

China, on the other hand, has developed regulations that balance both safety and data protection, ensuring that AVs meet strict standards before deployment.

These examples show that India can adopt a combination of global best practices while tailoring them to its own needs.

IV. ANALYSIS AND FINDINGS

Analysis of Data on Autonomous Vehicles in India

The study of autonomous vehicles in India reveals both opportunities and challenges. AVs rely heavily on data collection, including location data, behavioural data, and environmental information. While this data is essential for safe and efficient operation, it also creates risks related to privacy and misuse.

The integration of different types of data allows AVs to function effectively, but it also increases the possibility of unauthorized access or exploitation. This raises concerns about how data is managed and protected.

Privacy Risks Identified

One major concern is continuous surveillance, as AVs can track and record user movements over time. This creates detailed profiles of individuals, which may be used without their knowledge or consent.

Another issue is data overreach, where information collected for one purpose may be used for other unintended purposes, such as targeted advertising.

There is also a lack of proper consent mechanisms, making it unclear whether users fully understand how their data is being used.

Security Vulnerabilities

AVs are vulnerable to cyber threats due to their reliance on connectivity. Hackers may attempt to gain access to systems, leading to data breaches or even control over the vehicle.

Communication systems can be manipulated, and software vulnerabilities may result in system failures or incorrect responses. These risks highlight the need for strong cybersecurity measures.

Gaps in the Legal Framework

The analysis shows several gaps in the current legal system:
Lack of specific laws addressing AV technology
Insufficient clarity on consent and transparency
Weak cybersecurity standards

Addressing the Research Questions

The research finds that while Indian laws provide a basic framework for data protection, they are not fully equipped to handle the complexities of AV technology.
There are significant gaps, particularly in areas such as real-time data processing, consent mechanisms, and security standards.
To address these issues, there is a need for specific legal reforms that focus on AV technology and its unique challenges.

V. RECOMMENDATIONS AND CONCLUSION

Recommendations for Regulating Autonomous Vehicles in India

As India moves towards adopting and integrating autonomous vehicle (AV) technology, it becomes extremely important to establish a strong and well-structured regulatory framework. Such a framework must ensure that AVs operate safely, respect individual privacy, and contribute positively to society as a whole. The following recommendations are aimed at improving India's regulatory approach, particularly in areas like privacy, data protection, cybersecurity, and alignment with global standards.

Develop Specific Legislation for Autonomous Vehicles

E. Enact AV-specific laws

Objective: There is a clear need to introduce comprehensive legislation that specifically addresses all aspects of autonomous vehicle technology. This includes rules relating to data collection, processing, consent, storage, sharing, and overall data security.

Details: These laws should clearly define the roles and responsibilities of all stakeholders involved, including manufacturers, software developers, data processors, and end-users. In addition, the legislation should establish standards that ensure smooth interoperability between different AV systems and the infrastructure that supports them.

F. Define clear standards for consent and transparency

Consent Protocols: A proper framework must be created where consent for data collection is not only taken but is also informed and meaningful. Users should clearly understand what data is being collected, the purpose behind it, and how it will be used.

Transparency Measures: AV operators should be required to provide clear and accessible information regarding data usage, sharing practices, and any incidents of data breaches. Transparency should also extend to the functioning of algorithms, especially those that affect safety and privacy.

Enhance Data Protection and Privacy Measures

G. Adopt data minimization principles

Legislative Action: The principle of data minimization should be formally included in law, ensuring that only the data necessary for the functioning of AVs is collected.
Practical Application: Data should not be stored for longer than required. Any unnecessary data must either not be collected at all or should be deleted promptly after use.

H. Implement robust encryption and anonymization techniques

Data Security: Strong encryption methods must be used to protect data both during transmission and while stored, preventing unauthorized access to sensitive information.
Anonymization Practices: Proper guidelines should be developed to ensure that personal data collected by AVs is

anonymized in such a way that it cannot be traced back to individuals.

Establish Comprehensive Cybersecurity Frameworks

I. Create AV-specific cybersecurity standards

Cybersecurity Protocols: There should be strict cybersecurity guidelines specifically designed for AV systems. These should address possible vulnerabilities and include real-time threat detection and response systems.
Regulatory Compliance: Regular audits and compliance checks must be made mandatory to ensure that manufacturers and service providers follow these standards properly.

J. Develop a national cybersecurity protocol for AVs

Unified Framework: A national-level cybersecurity framework should be developed with the help of experts to address issues like data protection, system reliability, and emergency response.
Stakeholder Involvement: Both public and private sector stakeholders should be involved in designing and implementing these measures to ensure practical and effective solutions.

Institute Regulatory Bodies and Advisory Committees

K. Set up an Autonomous Vehicle Regulatory

Authority

Regulatory Oversight: An independent authority should be established to monitor the implementation of AV regulations. This body would be responsible for licensing, compliance checks, and safety certifications.
Public Safety and Innovation: The authority should maintain a balance between ensuring public safety and encouraging innovation within the AV sector.

L. Form advisory committeE

Expert Panels: Advisory committees consisting of experts from fields like technology, law, ethics, and public policy should be created to guide regulatory developments.
Feedback Mechanism: These committees should also include systems for receiving public feedback and incorporating global best practices into policy decisions.

Promote Public Awareness and Stakeholder Engagement

Conduct public awareness campaigns
Educational Initiatives: Awareness programs should be introduced to educate people about how AVs work, their benefits, and the risks involved, especially regarding privacy and data protection.
Community Involvement: Public participation should be encouraged in discussions about AV deployment, particularly in urban planning and transportation systems.

M. Engage with stakeholders

Inclusive Dialogue: A collaborative environment should be created where inputs from developers, policymakers, users, and privacy advocates are actively considered.
Policy Development: Stakeholder feedback should play an important role in shaping policies to ensure they are practical and balanced.

Encourage International Collaboration and Benchmarking

N. Participate in international forums

Global Engagement: India should actively participate in international discussions and forums related to AV technology to stay updated on global developments.
Collaborative Projects: Engaging in international research and testing initiatives can help improve AV systems and regulatory practices.

O. Benchmark against global standards

Regular Reviews: India should regularly compare its regulatory framework with global standards to identify areas of improvement.
Adaptation and Adoption: Successful international practices should be adapted to suit India's legal, cultural, and infrastructural conditions.

Conclusion

The recommendations outlined above aim to create a strong and adaptable regulatory system for autonomous vehicles in India. By addressing critical areas such as legal frameworks, cybersecurity, public awareness, and

international cooperation, India can ensure that AV technology is introduced in a safe and responsible manner. Such a framework will not only protect individual privacy and data security but also support innovation and technological growth. Ultimately, this balanced approach will help India move forward confidently in adopting autonomous vehicles while maintaining trust, safety, and ethical standards in society.

REFERENCES

Books & Academic Sources

1. Daniel J. Solove, Understanding Privacy (Harvard Univ. Press 2008).
2. Woodrow Barfield & Ugo Pagallo eds., Research Handbook on the Law of Artificial Intelligence (Edward Elgar 2018).
3. Ryan Calo et al. eds., The Oxford Handbook of Law, Regulation and Technology (Oxford Univ. Press 2017).
4. Jack M. Balkin, The Path of Robotics Law, 6 Calif. L. Rev. Cir. 45 (2015).

◆ Reports & Institutional Publications/ reports and internet help

1. Nat'l Highway Traffic Safety Admin., Automated Vehicles for Safety (U.S. Dep't of Transp.).
2. Organisation for Econ. Co-operation & Dev. (OECD), OECD Privacy Principles (2013).
3. European Comm'n, EUREKA Prometheus Project (1987–1995).
4. United Nations Econ. Comm'n for Europe (UNECE), Automated Vehicles Regulatory Framework.
5. Ministry of Housing and Urban Affairs, Smart Cities Mission, Gov't of India.
6. Soc'y of Automotive Eng'rs, Taxonomy and Definitions for Terms Related to Driving Automation Systems for On-Road Motor Vehicles, SAE Standard J3016.
7. Google, Self-Driving Car Project (2009).
8. Information Technology Act, No. 21 of 2000 (India).
9. Digital Personal Data Protection Act, No. 22 of 2023 (India).
10. Motor Vehicles Act, No. 59 of 1988 (as amended in 2019) (India).
11. Regulation (EU) 2016/679 of the European Parliament and of the Council (General Data Protection Regulation), 2016 O.J. (L 119) 1.