EYES ON THE ROAD, LAWS IN THE DARK: THE UNCERTAIN LEGALITY OF DASHCAMS IN INDIA

Krishna R, Sathyabama Institute of Science and Technology

ABSTRACT

More and more vehicle owners in India are installing dashboard cameras (dashcams) at an unprecedented level as road safety, personal security and video evidence gain importance. But this emerging technological change is playing out against a backdrop of complicated and dynamic legal processes. With the implementation of the Digital Personal Data Protection Act, 2023, India has started a new journey when it comes to the data privacy regime and this brings to the fore a key question about whether or not, dashcam usage in India falls within the law's scope. This article analyzes specific legal uncertainties in relation to dashcams under the new data protection regime, exploring issues such as consent, data processing, retention, and public dissemination of recorded footage. Comparative insights are drawn from jurisdictions such as the United Kingdom, United States, and European Union, where privacy jurisprudence has long shaped the contours of dashcam legality. In India, the intersection of the DPDP Act with constitutional rights under Article 21 and other statutory provisions such as the Information Technology Act and the Indian Penal Code adds layers of complexity. The paper highlights the need for explicit regulatory guidelines to balance the competing interests of personal security, public interest, and the fundamental right to privacy. Through this analysis, the study exposes the existing legal grey areas and underscores the necessity of judicial clarity and legislative precision in governing dashcam use in India.

Keywords: Dashcams; Data Privacy; Right to Privacy; Electronic Evidence; Consent; Public Dissemination; European Union GDPR; Personal Security; Road Safety; Technological Surveillance

I. INTRODUCTION

The rapid adoption of dashboard cameras, commonly known as dashcams, reflects a growing public interest in personal safety, evidentiary support in traffic disputes, and accountability on India's increasingly congested and unpredictable roads[1]. These compact devices, once a rarity, are now becoming standard accessories in private and commercial vehicles alike, capturing continuous audio-visual recordings of the road and its surroundings[2]. However, this technological advancement raises complex and evolving legal questions regarding privacy, consent, data protection, and evidentiary admissibility within the Indian legal system.

Until recently, India's legal landscape lacked a comprehensive statutory framework to regulate the collection, processing, and dissemination of personal data captured by such devices. This regulatory vacuum led to widespread uncertainty regarding the permissibility and scope of dashcam usage, particularly when such recordings inadvertently captured third parties—pedestrians, other drivers, and bystanders—without their knowledge or consent. However, with the recent enactment of the Digital Personal Data Protection Act, 2023 (DPDP Act), India has taken a significant legislative step toward codifying data privacy rights and obligations, thereby reshaping the legal environment in which dashcams operate.

The DPDP Act introduces statutory obligations on data fiduciaries and processors, which may extend to dashcam users, particularly when recordings are used beyond personal purposes—such as shared on social media, submitted as evidence, or disseminated commercially. Key principles such as purpose limitation, data minimization, notice requirements, and consent for processing identifiable personal data are now legally mandated, bringing India closer in alignment with global data protection regimes such as the European Union's General Data Protection Regulation (GDPR). Yet, practical questions remain unresolved: Does the private use of dashcams fall within the Act's ambit? Are vehicle owners considered data fiduciaries when recording in public spaces? How should incidental capture of non-consenting individuals be managed in compliance with the law?

This paper seeks to critically examine these uncertainties by exploring the intersection of dashcam technology, individual privacy rights, and India's emerging data protection

[1] *Rathi, A. (2023). "Growing adoption of dashcams in India: Trends and drivers." The Economic Times.* Retrieved from: https://economictimes.indiatimes.com

[2] *Vohra, A. (2022). "Why Dashcams Are Becoming a Necessity in India." India Today.* Retrieved from: https://www.indiatoday.in/auto/story/why-dashcams-are-necessary-in-india-1920834-2022-03-01

framework under the DPDP Act. In doing so, it aims to highlight the existing gaps, interpretative challenges, and potential judicial approaches that may define the legality and limits of dashcam usage in India's evolving digital and legal ecosystem**.**

II. THE LEGAL VACUUM: INDIAN STATUTES AND DASHCAMS

The increasing prevalence of dashcams in private and commercial vehicles across India has sparked pertinent legal concerns regarding their validity, regulation, and admissibility under the country's legal framework, which currently remains fragmented and incomplete in addressing such personal surveillance technologies. Central to this discourse is Article 21 of the Constitution of India, which guarantees the fundamental right to privacy, as firmly established in the landmark judgment of *Justice K.S. Puttaswamy v. Union of India (2017)*[3]. This judgment recognized privacy as a constitutionally protected right and importantly distinguished between the expectations of privacy in public and private spaces. Dashcams primarily record footage of public roads—spaces where the expectation of privacy is considerably lower. However, complications arise when these devices inadvertently capture visuals from private areas or record sensitive acts, thus posing a potential threat to privacy rights under Article 21. The Information Technology Act, 2000, specifically Section 66E, criminalizes the intentional capture, transmission, or publication of images of private areas without consent, offering some protection against privacy violations. Nevertheless, this provision falls short of addressing the incidental recording potential of dashcams and imposes no clear data security obligations on private individuals operating such devices, leaving a regulatory void concerning personal surveillance equipment used in public spaces[4]. Furthermore, the Indian Penal Code, 1860, becomes applicable where dashcam footage is misused; offences like voyeurism under Section 354C, defamation under Section 499, and extortion under Section 383 could be invoked if such recordings are exploited for malicious purposes like blackmail, harassment, or character damage. However, these IPC provisions merely address the consequences of misuse and fail to establish specific guidelines for the lawful and ethical usage of dashcams. In matters of evidentiary value, the Indian Evidence Act, 1872, particularly Sections 3 and 65B, recognizes electronic records, including dashcam

[3] *K.S. Puttaswamy v. Union of India*, (2017) 10 SCC 1.

[4] Dev Kaur (2024). *A Comparative Study of the Evaluation on the Right to Privacy in India and the UK, Their Legal Frameworks and Judicial Interpretation: A Cyber Law Perspective.* International Journal of Legal Science and Innovation (IJLSI).https://ijlsi.com/wp-content/uploads/A-Comparative-Study-of-the-Evaluation-on-the-Right-to-Privacy-in-India-and-the-UK-Their-Legal-Frameworks-and-Judicial-Interpretation.pdf

footage, as admissible evidence in legal proceedings, subject to conditions of authenticity and certification. The Supreme Court in *Ritesh Sinha v. State of UP*[5] reaffirmed the admissibility of such electronic evidence, provided compliance with Section 65B's procedural mandates is ensured. Thus, dashcam recordings can substantively support legal claims, such as those arising in road accident disputes or insurance claims, only when they meet these evidentiary prerequisites. Despite this, the Motor Vehicles Act, 1988, which governs the use and regulation of vehicles in India, remains conspicuously silent on the subject of dashcams; neither mandating nor prohibiting their installation or usage in private or commercial vehicles, thereby leaving their adoption and application to the discretion of vehicle owners without statutory guidance. This legal silence stands in stark contrast to jurisdictions like Russia or the United Kingdom, where the use of dashcams is either promoted or clearly regulated through specific policies[6]. In conclusion, although various Indian statutes—including constitutional provisions, the Information Technology Act, the Indian Penal Code, and the Indian Evidence Act—incidentally engage with issues arising from dashcam usage, there exists no cohesive or comprehensive legal framework that delineates the permissible scope, obligations, or restrictions associated with such devices. This legislative gap generates ambiguity for both dashcam users and individuals inadvertently recorded by such devices, underscoring the pressing need for a clear, structured regulatory regime to address the evolving realities of vehicular surveillance technologies in India.

III. PRIVACY, CONSENT, AND ETHICAL CHALLENGES

The use of dashcams and personal recording devices raises several pressing privacy, consent, and ethical challenges, particularly concerning the rights of bystanders inadvertently captured in such recordings. One of the foremost concerns is the lack of bystander consent, which holds significant implications under privacy jurisprudence. While individuals typically have a diminished expectation of privacy in public spaces, many data protection laws—such as the European Union's General Data Protection Regulation (GDPR) and California's Consumer Privacy Act (CCPA)[7]may still classify dashcam footage containing identifiable features (like

[5] *Ritesh Sinha v. State of UP*, (2019) 8 SCC 1.
[6] KV Brahmam & AOK Muppavaram (2023). *Data Privacy and Cyber Security in India: A Critical Examination of Current Legal Frameworks.* ResearchGate. Available at: https://www.researchgate.net/publication/383270800_CYBER_CRIME_Cyber_Securities_in_India
[7] *Akhlaghpour, S., Hassandoust, F., & Fatehi, F. (2021). Learning from Enforcement Cases to Manage GDPR Risks. MIS Quarterly Executive, 20(2), 115-134.* Available at: https://search.ebscohost.com/login.aspx?direct=true&db=bth&AN=152709663&site=ehost-live

faces or license plates) as personal data. This can potentially expose dashcam owners to legal liability if they collect, store, or share this data without proper legal justification or consent, especially if such recordings are retained unnecessarily or disseminated beyond their intended purpose.

A related and equally critical issue is the potential misuse of dashcam footage via social media dissemination, where content may be uploaded without consent or proper anonymization. Such actions risk defamation, harassment, and reputational harm to individuals inadvertently filmed. The viral nature of social media can amplify these harms, turning ordinary citizens into the subjects of public ridicule, misjudgment, or "trial by internet" without due process or context[8]. Moreover, out-of-context or selectively edited footage can lead to misleading narratives, giving rise to civil claims such as defamation or intentional infliction of emotional distress.

In light of these risks, dashcam owners bear an important set of ethical responsibilities. These include practicing data minimization by retaining footage only as long as necessary and securely deleting it thereafter to prevent privacy breaches. When sharing recordings publicly, ethical practice demands that owners blur faces, license plates, or any personally identifying information to safeguard the identities of uninvolved individuals, unless there is a legitimate public interest—such as reporting a crime[9]. Moreover, dashcam users should refrain from posting footage for entertainment or public shaming and must consider whether consent is needed from passengers or other recorded individuals, particularly in regions where informed consent for recording is legally mandated. These responsibilities underscore the balance that must be maintained between personal security interests and the broader public right to privacy and dignity.

IV. INTERNATIONAL LEGAL PERSPECTIVES

The legality and regulation of dashboard cameras (dashcams) present a varied global landscape, shaped predominantly by jurisdiction-specific approaches to privacy, data protection, and surveillance. In countries with established data protection regimes, dashcam usage is not only widespread but also heavily governed to balance technological benefits with the fundamental

[8] *Fan, M. D. (2022). The Hidden Harms of Privacy Penalties. UC Davis Law Review, 56(1), 117-178.* Available at: https://heinonline.org/HOL/P?h=hein.journals/davlr56&i=117

[9] *Visconti, P., Del-Valle-Soto, C., & Velázquez, R. (2025). Innovative Driver Monitoring Systems and On-Board Vehicle Devices in Smart-Road Scenarios. Sensors, 25(2), 562.*
Available at: https://www.mdpi.com/1424-8220/25/2/562

rights to privacy and data security. The passage of India's Digital Personal Data Protection Act, 2023 (DPDP Act) signals its readiness to align more closely with these international standards, yet critical distinctions remain when comparing India's emerging regulatory environment with other global jurisdictions.

In the European Union (EU), the General Data Protection Regulation (GDPR) represents one of the most stringent data privacy frameworks in the world. Dashcam usage in the EU is subject to strict conditions, including the requirement that recordings must serve a legitimate interest without unduly infringing upon the rights and freedoms of data subjects[10]. Member states like Austria have imposed near prohibitions on public dashcam use without prior authorization, reflecting a high sensitivity to bystander privacy. Similarly, in Germany, the Federal Court of Justice permits dashcam footage as court evidence only under exceptional circumstances where the public interest outweighs individual privacy rights. Non-compliance with GDPR mandates—including lack of consent, improper data retention, or unauthorized dissemination—can attract severe penalties, highlighting the regulatory rigor in the region.

The United Kingdom (UK), post-Brexit, has retained GDPR principles within its domestic data protection law via the UK GDPR and the Data Protection Act 2018. While private use of dashcams remains broadly permissible, commercial or public dissemination of footage invokes full data protection obligations. Dashcam operators must provide notice, ensure minimal data retention, and safeguard against unauthorized disclosure—requirements consistent with the broader European approach to personal data protection.

In contrast, the United States (US) adopts a sectoral and state-specific model, where dashcam regulation is fragmented and varies widely[11]. While video recording in public spaces is generally permissible due to a lower expectation of privacy, audio recording laws—such as two-party consent requirements in California and Connecticut—impose additional restrictions. Tort law doctrines like defamation, intrusion upon seclusion, and public disclosure of private facts govern improper dissemination of dashcam footage, but the absence of a unified federal data protection law creates inconsistency and legal uncertainty, particularly for interstate travelers and transport operators.

[10] European Union. (2016). *General Data Protection Regulation (GDPR) (EU) 2016/679.*
[11] Sinha, S. (2024). *Harmonizing Data Privacy Laws: A Comparative Study of Approaches in the EU, US and India.* Legal Spectrum Journal, 4. HeinOnline.
Available at: https://heinonline.org/hol-cgi-bin/get_pdf.cgi?handle=hein.journals/lglspuj4&section=5

India's introduction of the DPDP Act, 2023 marks a significant shift towards international convergence in data protection norms. The Act imposes core obligations such as obtaining consent before processing personal data, ensuring data minimization, purpose limitation, and the right of data principals to access and correct their data. These provisions bring India closer to GDPR-style protections, potentially affecting dashcam usage by requiring drivers and vehicle owners to inform passengers and bystanders (where practicable) about the operation of dashcams. Further, the dissemination of recorded footage—especially on social media or public platforms—may require anonymization or consent, akin to practices in the UK and EU. However, practical enforcement, public awareness, and judicial interpretation of these provisions in the dashcam context remain underdeveloped in India compared to the mature regulatory frameworks of Western jurisdictions.

Notably, countries such as Australia, Canada, and Japan also reflect diverse regulatory approaches. Australia's Privacy Act 1988 governs dashcam data when used in a business or commercial capacity but exempts personal use. Canada's Personal Information Protection and Electronic Documents Act (PIPEDA) requires organizations to obtain consent when recording identifiable individuals, while Japan's Act on the Protection of Personal Information (APPI) mandates strict handling of video data that identifies persons.

While India's enactment of the DPDP Act is a landmark step towards harmonization with global data privacy norms, its dashcam regulation remains in its infancy. International experience illustrates that effective dashcam governance requires not only statutory provisions but also clear judicial guidance, regulatory enforcement, and public compliance—a developmental trajectory that India must now undertake. The divergence and commonalities across jurisdictions underscore the complexities of balancing technological utility with individual privacy rights in the age of pervasive surveillance.

V. POLICY GAPS AND THE NEED FOR REGULATION (POST-DPDP ACT, 2023)

With the recent enactment of the Digital Personal Data Protection Act, 2023 (DPDP Act, 2023), India has finally taken a decisive step towards establishing a formal data protection regime aligned with global standards such as the European Union's GDPR. However, despite this progressive legislative development, significant policy gaps persist regarding the specific regulation of dashcam usage, revealing the urgent need for tailored guidelines in this niche but

rapidly expanding technological area. The DPDP Act, while laying down overarching principles of data processing, consent, and protection, does not directly address the unique challenges posed by personal surveillance devices like dashcams, leaving various operational and ethical issues unresolved.

One of the foremost concerns remains the conflict between public security interests and individual privacy rights. Dashcams are often promoted as tools for ensuring personal safety, recording accidents, and providing evidence in road disputes. However, indiscriminate or excessive recording—especially in sensitive areas such as private residences, gated communities, or non-consensual passenger recordings—could infringe upon the fundamental right to privacy under Article 21 of the Constitution, now reinforced by the privacy principles enshrined in the DPDP Act. The law does not currently specify whether dashcam operators, who capture personal data in the form of video and audio recordings, qualify as 'data fiduciaries' under the Act, nor does it clarify the extent to which consent from bystanders or passengers is required for such recordings. This regulatory ambiguity creates uncertainty for both users and enforcement agencies, potentially inviting misuse or abuse of such devices.

Another unresolved gap pertains to data storage, security, and retention policies concerning dashcam footage. Although the DPDP Act mandates that data fiduciaries must ensure the storage of personal data only for the period necessary for the specified purpose, no sector-specific standard has yet been formulated for dashcam recordings. Without clear timelines for data retention or requirements for secure storage (such as encryption), dashcam data remains vulnerable to unauthorized access, cyber theft, or misuse, undermining the very purpose of the data protection law. Further, lack of standardization regarding footage deletion policies risks unnecessary accumulation of sensitive data, increasing the potential for accidental disclosure or wrongful use.

A critical legal vacuum also exists regarding the admissibility and evidentiary status of dashcam recordings in judicial proceedings. While electronic records are generally admissible under the Indian Evidence Act, 1872, procedural clarity is absent concerning the authenticity, integrity, and chain of custody standards required for dashcam footage to be reliably used in courts or tribunals. The absence of procedural safeguards could result in the wrongful rejection of valid evidence or the misuse of tampered or selectively edited recordings in legal disputes. The DPDP Act does not address this evidentiary dimension, indicating the need for

supplementary judicial or legislative clarification to harmonize data protection obligations with the requirements of criminal and civil procedure.

Furthermore, the unrestricted online dissemination of dashcam content represents a serious lacuna that the DPDP Act alone does not remedy. While the Act prohibits processing and disclosure of personal data without consent, it remains unclear whether casual or non-commercial sharing—such as uploading dashcam videos on social media platforms—falls within its ambit when done by individuals rather than recognized data fiduciaries. The risk of reputational damage, harassment, defamation, or unauthorized exposure of private citizens persists unless specific restrictions are imposed on such sharing practices, including mandatory anonymization or blurring of identifiable features such as faces and vehicle registration numbers before public release[12].

In view of these enduring gaps, there is an undeniable need for sector-specific regulation or guidelines governing dashcam use in India. This regulatory framework should unambiguously define the permissible limits of recording in public versus private spaces, impose obligations regarding data storage, security, and erasure, lay down detailed norms for evidentiary admissibility of dashcam footage, and enforce strict controls on the public dissemination of recorded material. Only through such comprehensive and tailored measures can India effectively balance the twin objectives of technological utility and constitutional privacy protection, ensuring that dashcams serve their intended purpose without becoming tools of unregulated surveillance or personal rights violations. The passage of the DPDP Act, 2023, while a significant milestone, thus marks merely the beginning—not the culmination—of the regulatory journey in this evolving technological space.

VI. JUDICIAL TRENDS AND CASE ANALYSIS

The judicial discourse in India on the legality and regulation of dashcams remains largely underdeveloped, with courts yet to directly address issues relating to their deployment, permissible scope, and data protection obligations. However, certain landmark judgments and recent legislative developments offer foundational principles that are likely to influence any future adjudication in this space. The Supreme Court's decision in *Justice K.S. Puttaswamy*

[12] Hloviuk, I., Zavtur, V., & Zinkovskyy, I. (2024). The use of video and audio recordings provided by victims as evidence. *Social and Legal Studios*, 7(1), 145-154. https://sls-journal.com.ua/web/uploads/pdf/Social_and_Legal_Studios_Vol.7_No.1_2024-145-154.pdf

(Retd.) v. Union of India (2017) stands as the cornerstone in this context, where the right to privacy was elevated to the status of a fundamental right under Article 21 of the Constitution. The Court emphasized that individuals enjoy control over their personal information, including images or videos that could identify them in public or private settings. Although this judgment did not explicitly address dashcams, its broad interpretation of privacy rights suggests that indiscriminate or unauthorized recording and dissemination of dashcam footage—especially when it involves identifiable persons or private moments—could potentially violate constitutional protections unless justified by law, public interest, or necessity. Additionally, the Court's insistence on the principles of legality, necessity, and proportionality as prerequisites for any invasion of privacy indicates that future judicial scrutiny of dashcam practices would likely be guided by these standards, ensuring that privacy infringements are minimal, justified, and backed by legitimate purpose.

Further, the admissibility of dashcam footage as electronic evidence would be governed by principles laid down in cases such as *Ritesh Sinha v. State of Uttar Pradesh* (2019), where the Court affirmed the growing role of electronic records in legal proceedings. The ruling clarified that even in the absence of specific statutory provision, courts could exercise inherent powers to admit electronic evidence—provided such records comply with procedural requirements under Sections 65A and 65B of the Indian Evidence Act, 1872, which pertain to authenticity, integrity, and certification of digital data. This indicates that dashcam footage, if properly preserved and certified, could potentially be admitted as reliable evidence in criminal trials, motor accident claims, or civil disputes.

The enactment of the Digital Personal Data Protection (DPDP) Act, 2023 marks a significant statutory development in this regard. The Act introduces a comprehensive data protection regime by recognizing any visual or audio data that identifies an individual—including dashcam footage—as "personal data" subject to legal safeguards. Although personal or domestic use may be exempt, the moment such footage is shared publicly or processed for non-personal purposes (such as uploading accident videos on social media), obligations of consent, lawful processing, purpose limitation, and data security come into force. The Act mandates that data fiduciaries (including private individuals when sharing data beyond personal use) secure informed consent, minimize data collection to necessity, and prevent unauthorized disclosure—obligations that may render public dashcam footage legally questionable if these conditions are not met. However, no court has yet interpreted the DPDP Act in the context of

dashcams, leaving a judicial vacuum on how these obligations will be practically enforced.

Despite these constitutional and legislative developments, it is important to note that there is a conspicuous absence of any direct judicial ruling in India specifically addressing dashcam usage, its privacy implications, or its legal limits. No reported cases from the Supreme Court or High Courts have adjudicated on whether dashcam recording amounts to a breach of privacy, whether bystanders can claim violation of their rights, or how dashcam evidence should be treated in light of the new data protection law. This stands in contrast to jurisdictions like the European Union and the United Kingdom, where courts have evaluated dashcam use against stringent data protection regulations like the GDPR. The silence of Indian courts on these matters perpetuates a legal ambiguity that leaves dashcam users, data subjects, and law enforcement without clear judicial guidance.

In conclusion, while Indian courts have laid the groundwork for evaluating privacy rights and electronic evidence admissibility, the absence of dashcam-specific judicial interpretation creates an uncertain legal environment, especially after the introduction of the DPDP Act, 2023. It is expected that future litigation or legislative clarification will be necessary to resolve these ambiguities and to establish clear standards governing the responsible and lawful use of dashcams in India.

VII. RECOMMENDATIONS

The increasing prevalence of dashcams in private and commercial vehicles in India necessitates a well-defined, legally sound framework to address the associated privacy, data protection, and ethical concerns. In view of the present legislative and regulatory lacunae, several key recommendations may be advanced to guide policymakers, regulators, and stakeholders towards creating a balanced regime that safeguards both the public interest in safety and accountability, and the individual's fundamental right to privacy.

To begin with, India requires the formulation of a comprehensive statutory framework specifically addressing dashcam usage, either through the introduction of a standalone law or via appropriate amendments to the Motor Vehicles Act, 1988. This framework should clearly define the scope, limitations, and permissible purposes of dashcam use in both personal and commercial contexts. It must address issues such as the legality of in-cabin recording, mandatory disclosure of recording to passengers, the obligation to notify third parties (where

feasible) in public or semi-private spaces, and explicit prohibitions on misuse such as voyeuristic or defamatory recording practices.

Further, India's nascent data protection regime must be strengthened by integrating provisions modelled on the General Data Protection Regulation (GDPR) of the European Union, specifically in relation to dashcam data handling. Such provisions should require dashcam users—especially those sharing or disseminating footage beyond private use—to comply with principles of data minimization, purpose limitation, and storage limitation. Requirements such as the anonymization or masking of personally identifiable features (like faces, vehicle registration numbers, or private property) before public distribution should be made mandatory. Additionally, consent mechanisms must be introduced, especially in cases where dashcams record passengers inside vehicles or bystanders in spaces where they may have a reasonable expectation of privacy.

A parallel effort must be made to promote public awareness and dissemination of compliance guidelines. The general public—including private vehicle owners, cab aggregators, commercial fleet operators, and law enforcement agencies—must be educated about the legal obligations and ethical considerations involved in dashcam use. Government agencies, in collaboration with transport authorities and digital rights organizations, should issue clear and accessible guidance outlining what is permissible and what constitutes a violation under the proposed framework. Such guidelines could cover best practices for safe data handling, proper disclosure methods, responsible online sharing of footage, and procedures for deleting or archiving sensitive recordings after a reasonable period.

Finally, there is an urgent need to establish an effective and accessible grievance redressal mechanism to deal with complaints arising from dashcam misuse. Individuals who are recorded without consent and subsequently suffer harm—such as through unauthorized publication, defamation, harassment, or infringement of privacy—must have the right to approach specialized adjudicatory forums. These could take the form of dedicated cyber law benches, consumer protection courts, or data protection authorities empowered to award swift remedies, including takedown orders, monetary compensation, and punitive measures against offending parties. The establishment of such mechanisms will instill confidence in the public and provide a necessary check against the potential misuse of dashcam technology.

In sum, these recommendations underscore the importance of developing a holistic and

forward-looking legal and regulatory ecosystem in India that reflects the evolving interplay between personal safety technology and individual privacy rights. A well-calibrated dashcam policy, underpinned by clear legislation, robust data protection standards, public education, and enforceable accountability measures, will bridge the current gap and ensure that technological progress does not come at the cost of constitutional freedoms and civil liberties.

VIII. CONCLUSION

With the enactment of the Digital Personal Data Protection (DPDP) Act, 2023, India has taken a significant step toward establishing a comprehensive legal framework for personal data protection in the digital era. This legislative milestone marks a crucial shift in the governance of technologies such as dashcams, which, until recently, operated in a legal vacuum. Under the new law, dashcam users, particularly those whose recordings extend beyond personal use into public dissemination or commercial purposes, are now classified as data fiduciaries and are thus bound by statutory obligations relating to the collection, processing, storage, and disclosure of personal data captured through these devices.

The DPDP Act mandates that data fiduciaries must adhere to principles of purpose limitation, data minimization, and storage limitation, ensuring that dashcam footage is collected only for lawful and specific purposes—such as personal safety or evidentiary use—and is not retained beyond the necessary period. More importantly, the law enshrines the right of data principals (the individuals recorded) to be informed about the collection of their personal data and to exercise control over its usage, including the right to request deletion or restriction of processing. As a result, dashcam users are now legally required to implement measures such as anonymization of identifiable features (faces, license plates) when sharing footage publicly or on digital platforms, and to secure consent where required—particularly when capturing audio or recording in semi-private spaces.

Despite this regulatory advancement, challenges remain in ensuring widespread awareness and compliance, especially among private vehicle owners and small-scale commercial operators who may not be fully conversant with data protection obligations. The enforcement of these provisions will require a robust administrative mechanism, clear guidelines on permissible dashcam usage scenarios, and sector-specific codes of practice to avoid ambiguity. Moreover, the practical enforcement of individual rights—such as the right to erasure or correction of

data—may encounter logistical hurdles in cases where dashcam footage involves multiple data subjects or is recorded incidentally in public spaces.

Nevertheless, the DPDP Act has decisively filled the previous legal grey zone by embedding dashcam use within the broader matrix of India's data protection regime. This development brings India closer to global standards such as the General Data Protection Regulation (GDPR) of the European Union and the Data Protection Act of the United Kingdom, both of which have long imposed stringent obligations on personal data handlers, including those using surveillance and recording devices like dashcams.

Looking forward, it is imperative that supplementary rules or sectoral guidelines be issued under the DPDP framework to specifically address dashcam-related concerns. These should clarify issues such as informed notice requirements in vehicles, permissible duration of data retention, conditions for lawful disclosure to third parties (such as insurance companies or law enforcement agencies), and procedures for data breach reporting in the event of unauthorized access to dashcam footage. Additionally, public awareness campaigns and targeted educational efforts must be undertaken to ensure that dashcam users, both individual and corporate, are fully informed of their rights and duties under the new law.

In conclusion, while the Digital Personal Data Protection Act, 2023, provides long-overdue regulatory clarity and protection against the misuse of dashcam-generated data, the success of this framework will depend heavily on its effective implementation and the willingness of all stakeholders to comply with its mandates. Without such diligence, the twin objectives of technological benefit and privacy protection risk being undermined. Therefore, the integration of dashcam usage into India's data protection regime represents a critical opportunity to balance innovation with constitutional values—an opportunity that must be seized through continued legal refinement, enforcement, and public engagement.

REFERENCES

1. *Halder, D., & Basu, S. (2024). Digital dichotomies: Navigating non-consensual image-based harassment and legal challenges in India. Information & Communications Technology Law, 33(1), 112-129.* https://doi.org/10.1080/13600834.2024.2408914

2. *Jaydarifard, S., Yigitcanlar, T., & Paz, A. (2025). Risk factors and safety strategies for mitigating violations, harassment and assault in taxi and ride-hailing services. Transport Reviews, 45(3), 305-322.* https://doi.org/10.1080/01441647.2025.2512251

3. *Hong, R., & Zhuang, K. V. (2025). Producing value from injury: Dashcam platforms, accidents, and gig work. Social Media + Society, 11(2).* https://doi.org/10.1177/20563051251329083

4. *Singh, V., Raja, L., & Bhagirath, S. N. (2023). A review of parking slot types and their detection techniques for smart cities. Smart Cities, 6(5), 119.* https://www.mdpi.com/2624-6511/6/5/119

5. *Ministry of Electronics and Information Technology (MeitY), Government of India. (2023). The Digital Personal Data Protection Act, 2023.* https://www.meity.gov.in/content/digital-personal-data-protection-bill-2023

6. *European Union. (2016). General Data Protection Regulation (GDPR) Regulation (EU) 2016/679.* https://eur-lex.europa.eu/eli/reg/2016/679/oj

7. *Stemler, A., & Evans, J. W. (2025). Data privacy and the regulation of ridesharing platforms. American Business Law Journal, 62(1).* https://onlinelibrary.wiley.com/doi/abs/10.1111/ablj.12259

8. *Obioha, O. V., Selesi-Aina, O., & Kolade, T. M. (2024). Real-Time Data Governance and Compliance in Cloud-Native Robotics Systems. SSRN Electronic Journal.* https://papers.ssrn.com/sol3/papers.cfm?abstract_id=5018252