INTERNATIONAL JOURNAL FOR LEGAL RESEARCH AND ANALYSIS

Open Access, Refereed Journal Multi Disciplinary
Peer Reviewed

www.ijlra.com

ISSN: 2582-6433

DISCLAIMER

ISSN: 2582-6433

EDITORIALTEAM

EDITORS

Dr. Samrat Datta

Dr. Samrat Datta Seedling School of Law and Governance, Jaipur National University, Jaipur. Dr. Samrat Datta is currently associated with Seedling School of Law and Governance, Jaipur National University, Jaipur. Dr. Datta has completed his graduation i.e., B.A.LL.B. from Law College Dehradun, Hemvati Nandan Bahuguna Garhwal University, Srinagar, Uttarakhand. He is an alumnus of KIIT University, Bhubaneswar where he pursued his post-graduation (LL.M.) in Criminal Law and subsequently completed his Ph.D. in Police Law and Information Technology from the Pacific Academy of Higher Education and Research University, Udaipur in 2020. His area of interest and research is Criminal and Police Law. Dr. Datta has a teaching experience of 7 years in various law schools across North India and has held administrative positions like Academic Coordinator, Centre Superintendent for Examinations, Deputy Controller of Examinations, Member of the Proctorial Board

Dr. Namita Jain

Head & Associate Professor
School of Law, JECRC University, Jaipur Ph.D. (Commercial Law) LL.M., UGC-NET Post Graduation Diploma in Taxation law and Practice, Bachelor of Commerce.

Teaching Experience: 12 years, AWARDS AND RECOGNITION of Dr. Namita Jain are - ICF Global Excellence Award 2020 in the category of educationalist by I Can Foundation, India. India Women Empowerment Award in the category of "Emerging Excellence in Academics by Prime Time & Utkrisht Bharat Foundation, New Delhi. (2020). Conferred in FL Book of Top 21 Record Holders in the category of education by Fashion Lifestyle Magazine, New Delhi. (2020).Certificate of Appreciation for organizing and managing the Professional Development Training Program on IPR in Collaboration with Trade Innovations Services, Jaipur on March 14th, 2019

ISSN: 2582-6433

Mrs.S.Kalpana

Assistant professor of Law

Mrs.S.Kalpana, presently Assistant professor of Law, VelTech Rangarajan Dr.Sagunthala R & D Institute of Science and Technology, Avadi. Formerly Assistant professor of Law,Vels University in the year 2019 to 2020, Worked as Guest Faculty, Chennai Dr.Ambedkar Law College, Pudupakkam. Published one book. Published 8Articles in various reputed Law Journals. Conducted 1Moot court competition and participated in nearly 80 National and International seminars and webinars conducted on various subjects of Law. Did ML in Criminal Law and Criminal Justice Administration.10 paper presentations in various National and International seminars. Attended more than 10 FDP programs. Ph.D. in Law pursuing.

Avinash Kumar

Avinash Kumar has completed his Ph.D. in International Investment Law from the Dept. of Law & Governance, Central University of South Bihar. His research work is on "International Investment Agreement and State's right to regulate Foreign Investment." He qualified UGC-NET and has been selected for the prestigious ICSSR Doctoral Fellowship. He is an alumnus of the Faculty of Law, University of Delhi. Formerly he has been elected as Students Union President of Law Centre-1, University of Delhi. Moreover, he completed his LL.M. from the University of Delhi (2014-16), dissertation on "Cross-border Merger & Acquisition"; LL.B. from the University of Delhi (2011-14), and B.A. (Hons.) from Maharaja Agrasen College, University of Delhi. He has also obtained P.G. Diploma in IPR from the Indian Society of International Law, New Delhi. He has qualified UGC – NET examination and has been awarded ICSSR – Doctoral Fellowship. He has published six-plus articles and presented 9 plus papers in national and international seminars/conferences. He participated in several workshops on research methodology and teaching and learning.

ISSN: 2582-6433

ABOUT US

INTERNATIONAL JOURNAL FOR LEGAL RESEARCH & ANLAYSIS ISSN- 2582-6433 is an Online Journal is Monthly, Peer Review, Academic Journal, Published online, that seeks to provide an interactive platform for the publication of Short Articles, Long Articles, Book Review, Case Comments, Research Papers, Essay in the field of Law & Multidisciplinary issue. Our aim is to upgrade the level of interaction and discourse about contemporary issues of law. We are eager to become a highly cited academic publication, through quality contributions from students, academics, professionals from the industry, the bar and the bench. INTERNATIONAL JOURNAL FOR LEGAL RESEARCH & ANALYSIS ISSN 2582-6433 welcomes contributions from all legal branches, as long as the work is original, unpublished and is in consonance with the submission guidelines.

ISSN: 2582-6433

VEHICLE-TO-EVERYTHING (V2X) LEGAL GOVERNANCE FRAMEWORKS

AUTHORED BY - AMAN KUMAR JHA,
SUJAL CHHAJED & TANISHK BHAWSAR
National Law Institute University, Bhopal

ABSTRACT

The emergence of Vehicle-to-Everything (V2X) communication technology represents a paradigmatic shift in automotive cybersecurity governance, necessitating unprecedented legal frameworks that transcend traditional regulatory boundaries. This comprehensive analysis examines India's evolving V2X legal architecture, centering on the convergence of the Digital Personal Data Protection Act 2023, AIS-189 cybersecurity standards, and emerging spectrum allocation policies. Through comparative analysis with global regulatory regimes including the EU's UNECE R155, America's DSRC-to-C-V2X transition framework, and China's integrated cybersecurity approach, this research identifies critical governance gaps and proposes innovative legal solutions for cross-jurisdictional V2X deployment. The study reveals that India's consent-centric privacy framework, combined with its phased cybersecurity implementation timeline, positions the nation to potentially lead in developing adaptive V2X governance models that balance technological innovation with robust data protection. Key findings indicate that successful V2X legal harmonization requires novel approaches to real-time cross-border data governance, dynamic spectrum sharing frameworks, and multi-stakeholder liability allocation mechanisms that current legal architectures inadequately address.

Keywords: Vehicle-to-Everything (V2X), cybersecurity, legal frameworks, data protection, cross-border governance.

1. INTRODUCTION

Vehicle-to-Everything (V2X) technology fundamentally transforms the automotive landscape by enabling real-time communication between vehicles, infrastructure, pedestrians, and networks, creating an interconnected transportation ecosystem that operates beyond traditional legal boundaries. As connected and autonomous vehicles transition from experimental

ISSN: 2582-6433

technologies to commercial deployment, the legal frameworks governing V2X communications have become critical determinants of successful implementation, particularly in complex regulatory environments like India.

The V2X ecosystem encompasses multiple communication paradigms: Vehicle-to- Vehicle (V2V) for collision avoidance and traffic coordination, Vehicle-to- Infrastructure (V2I) for smart traffic management, Vehicle-to-Pedestrian (V2P) for vulnerable road user protection, and Vehicle-to-Network (V2N) for cloud-based services integration. Each communication type generates distinct legal challenges related to cybersecurity, privacy protection, spectrum allocation, and cross- jurisdictional governance.

India's approach to V2X legal governance is particularly significant because it represents the world's largest democracy attempting to balance rapid technological adoption with comprehensive data protection, while serving as a potential model for other emerging economies. The convergence of India's Digital Personal Data Protection Act 2023 (DPDP[1], Automotive Industry Standard AIS-189[2] cybersecurity requirements, and Draft National Telecom Policy 2025[3] spectrum frameworks creates a unique regulatory matrix that demands innovative legal solutions.

2. INDIA'S V2X CYBERSECURITY STANDARDS FRAMEWORK

2.1 The AIS-189 Cybersecurity Architecture

India's automotive cybersecurity governance centres on Automotive Industry Standard AIS-189, which mandates comprehensive Cyber Security Management Systems (CSMS) for all connected vehicles by October 2027. This standard, developed by the Automotive Research Association of India (ARAI) in collaboration with global automotive manufacturers, specifically addresses V2X communication security through multi-layered protection mechanisms.

The AIS-189 framework requires manufacturers to implement Security by Design principles throughout the vehicle development lifecycle, incorporating V2X- specific

[1] Digital Personal Data Protection Act, 2023 (22 of 2023).
[2] Automotive Research Association of India, *Automotive Industry Standard AIS-189: Approval of Vehicles with Regards to Cyber Security and Cyber Security Management System* (April 2024).
[3] Ministry of Communications, Government of India, *Draft National Telecom Policy (NTP), 2025* (24 July 2025) < https://dit.py.gov.in/sites/default/files/draftntp2025.pdf> accessed [15 July 2025].

ISSN: 2582-6433

security measures including Public Key Infrastructure (PKI) management, Hardware Security Module (HSM) integration, and Security Credential Management Systems (SCMS) for V2X communications. This approach aligns with international standards while addressing India's unique automotive ecosystem challenges, including extensive Tier 2 and Tier 3 supplier networks that must achieve cybersecurity compliance.

The intersection between AIS-189 requirements and V2X real-time communication security presents unprecedented challenges for legal liability attribution. When V2X security credentials are compromised across multiple jurisdictions during cross-border travel, determining responsibility between original equipment manufacturers, certificate authorities, and infrastructure providers requires novel legal frameworks that current product liability law inadequately addresses.

2.2 Comparative Global Cybersecurity Standards Analysis

European Union's UNECE R155[4] Approach: The EU's framework emphasizes whole vehicle lifecycle cybersecurity, requiring type approval authorities to verify cybersecurity management systems before market entry. For V2X communications, this includes mandatory certificate management, intrusion detection systems, and forensic logging capabilities. The EU approach provides greater regulatory certainty but may limit innovation through prescriptive requirements.

United States' Industry-Led Framework: The US Federal Communications Commission's recent transition from DSRC to C-V2X technology, mandated by 2024 orders, demonstrates a market-driven approach where industry develops security standards with minimal regulatory prescription. This creates flexibility but potentially inconsistent security implementations across manufacturers.

China's Integrated National Cybersecurity Model: China's approach integrates V2X cybersecurity with national cybersecurity laws, requiring data localization and state oversight of critical automotive data. This provides comprehensive security but limits international interoperability.[5]

[4] UNECE Global Technical Regulation No. 155 - Cybersecurity and Cybersecurity Management System.
[5] China Automotive Technology and Research Center, *'C-V2X Standardisation Progress'* (2023) <http://www.catrc.cn/> accessed [01 July 2025].

ISSN: 2582-6433

India's Balanced Approach: India's AIS-189 framework combines mandatory cybersecurity requirements with implementation flexibility, allowing manufacturers to choose specific technologies while meeting performance-based security objectives. This hybrid approach potentially enables innovation while ensuring baseline security standards.

2.3 V2X Certificate Management Legal Frameworks

The deployment of V2X-enabled vehicles requires sophisticated certificate management ecosystems where vehicles, infrastructure, and service providers continuously exchange security credentials to verify communication authenticity. AUTOCRYPT's development of India-compliant V2X security certification systems positions India among only five countries with comprehensive V2X certificate management frameworks.[6]

Cross-border V2X certificate recognition presents novel jurisdictional challenges. When an Indian vehicle with AIS-189 compliant certificates communicates with infrastructure in neighbouring countries using different certificate standards, legal frameworks must address mutual recognition agreements, certificate authority liability, and revocation procedures across jurisdictional boundaries.

3. INDIA'S V2X PRIVACY GOVERNANCE UNDER THE DIGITAL PERSONAL DATA PROTECTION ACT

3.1 DPDP Act Application to V2X Data Processing

India's Digital Personal Data Protection Act 2023 establishes a consent-centric framework for personal data processing that presents unique challenges for V2X communications. Unlike traditional data collection scenarios, V2X systems continuously generate and exchange data in real-time, including location information, driving behaviour patterns, and vehicle performance metrics that can constitute personal data under the DPDP Act.

The Act's consent requirements become particularly complex in V2X contexts involving multiple data subjects (drivers, passengers, pedestrians), shared vehicles, and cross-border data flows. The DPDP Act requires explicit consent for data processing, but V2X safety functions may require immediate data exchange without time for consent procedures, creating tension between legal compliance and functional requirements.

[6] AUTOCRYPT, *'India-Compliant V2X Security Certification Management System*' (AUTOCRYPT Blog, 28 March 2025) <https://autocrypt.io/india-compliant-v2x-scms> accessed 13 August 2025.

ISSN: 2582-6433

Developing dynamic consent mechanisms for V2X systems that can provide legally valid consent while maintaining real-time operational capability. This requires novel approaches to consent that may include algorithmic consent management, contextual consent frameworks, and emergency override provisions for safety-critical V2X communications.

3.2 V2X Data Minimization and Purpose Limitation

The DPDP Act's data minimization principle requires processing only data that is "necessary" for specified purposes. V2X systems collect extensive data for various functions including traffic optimization, predictive maintenance, emergency response, and commercial services, creating challenges in determining what constitutes "necessary" data processing.

Establishing legal standards for V2X data collection that satisfy DPDP Act requirements while enabling advanced transportation services. This involves developing purpose-specific data collection frameworks where different V2X functions (safety, traffic management, commercial services) operate under distinct data processing authorities with appropriate legal protections.

3.3 Cross-Border V2X Data Transfer Governance

V2X communications inherently involve cross-border data transfers as vehicles travel across state and international boundaries while maintaining continuous communication with various infrastructure and service providers. The DPDP Act permits international data transfers to countries with "adequate data protection standards" but doesn't specify how this applies to real-time vehicular data or temporary cross-border presence.

Comparative Global Privacy Approaches:

European GDPR[7] Model: Provides adequacy decisions and binding corporate rules for cross-border transfers but requires explicit mechanisms for V2X data processing under legitimate interests or vital interests' legal bases.

California Consumer Privacy Act (CCPA)[8]: Focuses on opt-out rights for data sales but provides limited frameworks for real-time cross-border data processing required by V2X systems.

China's Personal Information Protection Law (PIPL)[9]: Requires data localization with

[7] Regulation (EU) 2016/679 (General Data Protection Regulation) arts 45–49.
[8] *California Consumer Privacy Act* (Cal. Civ. Code §§ 1798.100–1798.199, 2018).
[9] *Personal Information Protection Law of the People's Republic of China* (adopted 20 August 2021, effective 1 November 2021).

ISSN: 2582-6433

limited exceptions for cross-border transfers, creating challenges for international V2X interoperability.

India's Emerging Approach: The DPDP Act's flexibility in cross-border transfer mechanisms, combined with potential sectoral regulations for automotive data, may enable more adaptive frameworks for V2X data governance than prescriptive localization requirements.

4. INDIA'S V2X SPECTRUM GOVERNANCE AND INFRASTRUCTURE POLICY FRAMEWORK

4.1 Spectrum Allocation Architecture for V2X Communications

India's National Frequency Allocation Plan 2022 (NFAP-2022) and National Telecom Policy 2025 establish the regulatory foundation for V2X spectrum governance, though specific spectrum delicensing for V2X communications remains under development. The 5.9 GHz band, globally recognized for V2X communications, requires coordination between automotive applications and existing telecommunications services.

The National Telecom Policy 2025 emphasizes dynamic spectrum sharing, spectrum leasing, and trading mechanisms that could enable more efficient V2X deployment compared to traditional dedicated spectrum allocation approaches. This policy framework positions India to potentially lead in innovative spectrum governance for emerging technologies.

Technical Challenge: India's diverse telecommunications ecosystem, including extensive mobile networks and emerging 5G deployment, requires coexistence frameworks where V2X communications operate alongside other spectrum users without interference. Legal frameworks must address priority mechanisms, interference resolution procedures, and spectrum coordination protocols across different service types.

4.2 Comparative Global Spectrum Approaches

China's Dedicated Allocation Model: Allocated 20 MHz in the 5.9 GHz band specifically for C-V2X communications, providing certainty for automotive manufacturers but potentially limiting spectrum efficiency.[10]

[10] *Personal Information Protection Law of the People's Republic of China* (adopted 20 August 2021, effective 1 November 2021).

ISSN: 2582-6433

European Coordinated Approach: Allocated 50 MHz in the 5.855-5.905 GHz band with standardized message formats through ETSI ITS standards, enabling cross-border interoperability while maintaining national implementation flexibility.[11]

United States' Transition Framework: The FCC's mandated transition from DSRC to C-V2X in the 5.9 GHz band, completed by 2024 orders, demonstrates regulatory adaptation to technological evolution while maintaining spectrum allocation.[12]

India's Adaptive Framework Potential: India's emphasis on spectrum sharing and dynamic allocation could enable more flexible V2X deployment that adapts to varying geographic and technological requirements across the country's diverse transportation infrastructure.[13]

4.3 V2X Infrastructure Deployment Legal Frameworks

V2X implementation requires extensive Roadside Unit (RSU) deployment across India's highway and urban infrastructure, involving coordination between central government, state authorities, and private infrastructure providers. The legal frameworks governing RSU deployment, maintenance, and liability allocation remain underdeveloped.

India's Smart Cities Mission[14] provides a framework for integrating V2X infrastructure with broader urban technology deployment but requires specific legal mechanisms for public-private partnership arrangements, data sharing agreements, and liability allocation between government infrastructure and private vehicle communications.

5. MULTI-STAKEHOLDER LIABILITY ALLOCATION IN V2X ECOSYSTEMS

5.1 Complex Stakeholder Ecosystem Governance

V2X systems involve unprecedented numbers of stakeholders with interconnected responsibilities: vehicle manufacturers providing V2X hardware and software, infrastructure providers managing roadside communications units, telecommunications companies providing cellular connectivity for C- V2X, certificate authorities managing security credentials, map and service providers supplying real-time information, and government entities maintaining traffic management systems.

[11] ETSI, 'Intelligent Transport Systems (ITS); Access layer specification for Intelligent Transport Systems operating in the 5 GHz frequency band' EN 302 663 V1.2.1 (2019).
[12] Federal Communications Commission, 'Report and Order and Further Notice of Proposed Rulemaking' FCC 20-22 (2020).
[13] National Frequency Allocation Plan 2022, Ministry of Communications.
[14] Ministry of Housing and Urban Affairs, Government of India, *Smart Cities Mission* (launched 2015).

ISSN: 2582-6433

Traditional product liability frameworks, designed for discrete product failures, become inadequate when addressing emergent system behaviours that arise from complex V2X ecosystem interactions. Legal frameworks must develop new concepts of collective responsibility, proportional liability allocation, and shared duty of care among ecosystem participants.

When V2X system failures result from interactions between multiple stakeholders' systems rather than individual component failures, determining liability requires innovative legal approaches. For example, when a traffic management system's algorithm conflicts with a vehicle manufacturer's collision avoidance system, causing an accident, legal frameworks must address algorithmic interaction liability that current law doesn't anticipate.

5.2 India-Specific Liability Considerations

India's unique traffic environment, featuring mixed vehicle types (cars, motorcycles, auto-rickshaws, bicycles) and heterogeneous technology adoption rates, creates additional liability complexities for V2X systems. V2X-enabled vehicles must interact with non-connected vehicles and vulnerable road users, requiring legal frameworks that address asymmetric information scenarios and graduated duty of care based on technology capabilities.

Developing India-specific V2X liability frameworks that account for the country's diverse transportation ecosystem while enabling advanced safety features. This includes multi-modal interaction standards, technology-dependent duty of care, and graduated liability allocation based on vehicle connectivity capabilities.

6. CROSS-JURISDICTIONAL V2X GOVERNANCE AND INTERNATIONAL HARMONIZATION

6.1 Border Crossing Legal Frameworks

V2X communications present unprecedented challenges for cross-border vehicle travel, as vehicles must transition between different regulatory frameworks, spectrum allocations, and security certificate systems while maintaining continuous safety communications. India's extensive land borders with Pakistan, China, Bangladesh, Nepal, Sri Lanka, and Myanmar require specific legal mechanisms for V2X interoperability agreements and cross-border incident response protocols.

ISSN: 2582-6433

European 5G-CroCo and 5G-MOBIX [15]projects demonstrate technical feasibility of cross-border V2X communications but reveal significant legal challenges in liability attribution, data sovereignty, and regulatory compliance when vehicles operate across multiple jurisdictions.

The complexity of India's geopolitical relationships requires sophisticated legal frameworks for V2X communications that may involve national security considerations, data localization requirements, and technology transfer restrictions while maintaining safety communication capabilities.

6.2 International Standards Harmonization

ISO/SAE 21434[16] Global Implementation: The international cybersecurity standard provides a foundation for global V2X security harmonization, but implementation varies significantly across jurisdictions. India's approach through AIS-189 demonstrates adaptation of global standards to local regulatory and industrial contexts.

UNECE Working Party WP.29 Influence[17]: The United Nations Economic Commission for Europe's automotive regulations, including cybersecurity and automated driving provisions, provide frameworks for international harmonization that India is increasingly adopting through AIS standards.

Bilateral and Multilateral Cooperation Frameworks: Developing legal mechanisms for mutual recognition of V2X certifications, cross-border incident response protocols, and shared cybersecurity threat intelligence among countries implementing V2X systems.

7. REGULATORY INNOVATION AND ADAPTIVE GOVERNANCE FOR V2X

7.1 Regulatory Sandbox Frameworks[18]

The rapid evolution of V2X technology requires adaptive regulatory approaches that can accommodate technological uncertainty while maintaining safety and security standards. Regulatory sandboxes provide controlled environments for testing innovative V2X applications with temporary regulatory relief and liability protection.

The potential for establishing V2X regulatory sandboxes that enable testing of advanced

[15] European Commission, *5G-CroCo* and *5G-MOBIX* Projects, Horizon 2020 Research and Innovation Programme (2020–2023).
[16] ISO/SAE 21434:2021 - *Road vehicles - Cybersecurity engineering* (adopted 31 August 2021).
[17] UNECE WP.29 regulations on vehicle cybersecurity <https://unece.org/transport/vehicle-regulations/wp29> accessed [22 July 2025].
[18] Ministry of Electronics and Information Technology, *'Framework for Regulatory Sandbox in India'* (2023).

ISSN: 2582-6433

applications like autonomous vehicle coordination, dynamic traffic optimization, and emergency vehicle priority systems while developing appropriate legal frameworks for commercial deployment.

7.2 Anticipatory Governance Models

V2X technology evolution requires legal frameworks that can anticipate and adapt to technological developments rather than reactively addressing them after deployment. Anticipatory governance approaches involve technology foresight, stakeholder engagement, and adaptive regulation that evolves with technological capabilities.

As V2X systems increasingly incorporate artificial intelligence for traffic optimization and safety management, legal frameworks must address algorithmic accountability, automated decision-making standards, and AI system certification for safety-critical applications.

8. Implementation Strategy and Compliance Frameworks

8.1 Phased Implementation Legal Architecture

India's diverse automotive market, ranging from low-cost vehicles to luxury connected vehicles, requires differentiated compliance approaches that enable V2X adoption across market segments while maintaining safety standards. Tiered implementation strategies could provide different requirements for different vehicle categories, price points, and use cases.

Incorporating V2X capabilities into Bharat New Car Assessment Program (Bharat NCAP)[19] safety ratings could incentivize adoption while providing consumer information about V2X capabilities.

8.2 Industry Collaboration and Standards Development

Successful V2X legal implementation requires extensive industry-government collaboration for standards development, testing protocols, and compliance verification. India's automotive industry association involvement in AIS standards development demonstrates effective stakeholder engagement models.

Establishing legal-technical working groups that combine automotive engineers, cybersecurity experts, legal professionals, and policy makers to develop implementable V2X governance

[19] Ministry of Road Transport and Highways, Government of India, *Bharat New Car Assessment Program (Bharat NCAP)* (launched 2022).

ISSN: 2582-6433

frameworks.

9. Future Research Directions and Legal Innovation Opportunities

9.1 Emerging Technology Integration

As quantum computing threatens current cryptographic systems, V2X legal frameworks must anticipate quantum-resistant security requirements, certificate migration protocols, and liability frameworks for quantum threat scenarios.[20]

The potential integration of brain-computer interfaces with V2X systems for enhanced driver awareness and automated vehicle control requires novel legal frameworks for cognitive consent, neural data protection, and mind-machine interface liability.

9.2 Sustainable Mobility Legal Frameworks

Electric Vehicle V2X Integration: The convergence of Vehicle-to-Grid (V2G) communications with V2X safety systems requires legal frameworks that address energy trading, grid stability responsibilities, and dual-use infrastructure governance.

As Mobility-as-a-Service (MaaS) platforms integrate V2X-enabled vehicles, legal frameworks must address multi-user consent, shared liability allocation, and platform responsibility for V2X system maintenance and security.

10. Conclusions and Recommendations

This comprehensive analysis highlights that India's approach to Vehicle-to-Everything (V2X) legal governance presents a significant opportunity to pioneer innovative frameworks that effectively balance rapid technological advancement with robust privacy protections and stringent cybersecurity requirements. The intersection of the Digital Personal Data Protection Act's consent-centric privacy provisions, the adaptive cybersecurity standards embodied in Automotive Industry Standard AIS-189, and the forward-looking spectrum management policies outlined in the National Telecom Policy 2025 uniquely position India to assume a leadership role in shaping global V2X governance paradigms.

India's distinctive position is underscored by its expansive automotive market, multifaceted and diverse traffic ecosystem, and a regulatory environment characterized by flexibility and adaptability. This confluence creates fertile ground for the development of V2X governance

[20] K Shilton, *'Legal Models for Post-Quantum Cryptography'* (2024) 14(3) Int J Law Info Tech 191.

ISSN: 2582-6433

models that are not only tailored to India's unique context but also hold applicability as benchmarks for other emerging economies navigating similar technological transitions.

The inherently international and border-transcending nature of V2X technology introduces an imperative for unprecedented levels of cross-jurisdictional cooperation. Effective governance will require the establishment of mechanisms for legal harmonization, mutual recognition of security certifications, and coordinated incident response frameworks, addressing challenges that transcend traditional national legal boundaries.

Current product liability doctrines are insufficient to address the complex, interconnected V2X ecosystem where responsibility is distributed across multiple stakeholders including manufacturers, infrastructure providers, telecommunications operators, and software developers. These realities necessitate fundamental revisions to liability frameworks to accommodate shared duty of care and collective accountability within this multifaceted technological ecosystem.

Moreover, the rapid pace of innovation in V2X technologies demands governance models that are dynamic and capable of evolving in tandem with technological progress. Regulatory approaches must be flexible yet rigorous enough to maintain consistent standards of safety, security, and public trust over time.

From a strategic perspective, Indian policymakers are advised to prioritize the establishment of bilateral cooperation agreements with neighbouring countries to facilitate seamless cross-border V2X communications. The creation of regulatory sandbox frameworks would enable the testing and refinement of novel V2X applications while providing defined protections against liability risks. Additionally, forming multi-stakeholder governance bodies involving automotive manufacturers, telecommunications providers, and civil society is essential for inclusive and effective oversight.

On the global stage, the formation of international V2X treaty frameworks akin to aviation safety agreements can drive the coordination of cross-border V2X operations. Mechanisms for mutual recognition of V2X security certifications and shared cybersecurity threat intelligence platforms will be crucial to managing the global security landscape of connected transportation networks.

ISSN: 2582-6433

Future research trajectories should encompass the development of quantum-safe V2X security frameworks to address emerging cryptographic vulnerabilities, AI-integrated V2X governance models to accommodate increasing vehicular autonomy, and sustainable mobility legal frameworks that weave V2X technologies into broader environmental and energy policy objectives.

Ultimately, the success of V2X technology implementation hinges not only on technical innovation but equally on the sophistication of legal frameworks capable of governing complex, interconnected, and rapidly evolving technological systems. India's balanced approach of fostering innovation while safeguarding privacy and security offers valuable lessons for the global community. The challenges identified underscore the critical and ongoing need for legal innovation in this dynamic field.

The future of connected and autonomous transportation depends on legal frameworks that can evolve as rapidly as the technologies they regulate, necessitating unprecedented collaboration between technical and legal experts to ensure that the immense benefits of V2X technology can be realized without compromising privacy, security, or public safety.