# 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

# ABOUT US

The *International Journal for Legal Research & Analysis (IJLRA)* (ISSN: 2582-6433) is a peer-reviewed, academic, online journal published on a monthly basis. The journal aims to provide a comprehensive and interactive platform for the publication of original and high-quality legal research.

IJLRA publishes Short Articles, Long Articles, Research Papers, Case Comments, Book Reviews, Essays, and interdisciplinary studies in the field of law and allied disciplines. The journal seeks to promote critical analysis and informed discourse on contemporary legal, social, and policy issues.

The primary objective of IJLRA is to enhance academic engagement and scholarly dialogue among law students, researchers, academicians, legal professionals, and members of the Bar and Bench. The journal endeavours to establish itself as a credible and widely cited academic publication through the publication of original, well-researched, and analytically sound contributions.

IJLRA welcomes submissions from all branches of law, provided the work is original, unpublished, and submitted in accordance with the prescribed submission guidelines. All manuscripts are subject to a rigorous peer-review process to ensure academic quality, originality, and relevance.

Through its publications, the *International Journal for Legal Research & Analysis* aspires to contribute meaningfully to legal scholarship and the development of law as an instrument of justice and social progress.

ISSN: 2582-6433

# *PUBLICATION ETHICS, COPYRIGHT & AUTHOR RESPONSIBILITY STATEMENT*

The *International Journal for Legal Research and Analysis (IJLRA)* is committed to upholding the highest standards of publication ethics and academic integrity. All manuscripts submitted to the journal must be original, unpublished, and free from plagiarism, data fabrication, falsification, or any form of unethical research or publication practice. Authors are solely responsible for the accuracy, originality, legality, and ethical compliance of their work and must ensure that all sources are properly cited and that necessary permissions for any third-party copyrighted material have been duly obtained prior to submission. Copyright in all published articles vests with IJLRA, unless otherwise expressly stated, and authors grant the journal the irrevocable right to publish, reproduce, distribute, and archive their work in print and electronic formats. The views and opinions expressed in the articles are those of the authors alone and do not reflect the views of the Editors, Editorial Board, Reviewers, or Publisher. IJLRA shall not be liable for any loss, damage, claim, or legal consequence arising from the use, reliance upon, or interpretation of the content published. By submitting a manuscript, the author(s) agree to fully indemnify and hold harmless the journal, its Editor-in-Chief, Editors, Editorial Board, Reviewers, Advisors, Publisher, and Management against any claims, liabilities, or legal proceedings arising out of plagiarism, copyright infringement, defamation, breach of confidentiality, or violation of third-party rights. The journal reserves the absolute right to reject, withdraw, retract, or remove any manuscript or published article in case of ethical or legal violations, without incurring any liability.

ISSN: 2582-6433

# LEGAL CHALLENGES OF IOT IN INDIA: ASSESSING THE NECESSITY OF A CYBER INSURANCE MANDATE

AUTHORED BY - PRIYANGA P & NANDINI G

## *ABSTRACT*[1]

*The rapid proliferation of the Internet of Things (IoT) in India, spanning smart cities, industrial automation (IIoT), and connected healthcare, has outpaced existing risk management protocols. While the Digital Personal Data Protection Act 2023 provides a stringent penalty framework for data breaches, it lacks a specialised mechanism for the kinetic and physical risks unique to IoT ecosystems. Traditional cyber insurance policies in India, largely modelled on data-centric IT environments, are ill-equipped to address the complexities of IoT, such as software-tethering, multi-party attribution, and hardware-driven bodily harm. This research identifies a critical Protection Gap in the Indian insurance landscape. Through a comparative analysis of the IRDAI's current guidelines and international standards like the EU Cyber Resilience Act, the study evaluates the actuarial and legal hurdles in pricing IoT risks. Key challenges examined include the Zombie Device phenomenon, unpatched legacy hardware, and the shift from Information Liability to Physical Product Liability. The paper concludes by proposing a Unified IoT Cyber Insurance Framework. This model suggests a shift toward Secure-by- Design premium incentives and a statutory Safety Fund for SMEs. Ultimately, the research argues that a robust insurance framework is not merely a financial tool but a necessary pillar for India's digital sovereignty and consumer safety in a hyper-connected era.*

**Keywords:** *Internet of Things (IoT), Cyber Insurance, DPDP Act, IRDAI, Kinetic Risk, Product Liability,*

[1] ***Priyanga P*** *(PG Student) at School of Excellence in Law, Tamil Nadu Dr Ambedkar Law University, Chennai.*
***Nandini G*** *(PG Student) at School of Law, Hindustan Institute of Technology and Science, Chennai.*

ISSN: 2582-6433

# 1. INTRODUCTION

This year marks a watershed moment for India's digital transformation. With the nationwide rollout of 6G testing phases and the ubiquity of 5G-enabled infrastructure, the Internet of Things has transitioned from a luxury to a systemic necessity. From Smart Cities managing urban traffic to Connected Healthcare, systems monitoring patient vitals in real-time, the integration of physical hardware with cloud-based intelligence is now seamless.

However, this hyper-connectivity has birthed a sophisticated breed of vulnerabilities. Unlike traditional cyber threats that primarily target data integrity, IoT-based risks possess a kinetic dimension where a digital breach can result in physical devastation, such as a compromised smart grid causing a localised blackout or a hacked industrial sensor leading to factory-wide mechanical failure.

In this landscape, the Digital Personal Data Protection (DPDP) Act 2023 serves as a robust shield for personal data, imposing stringent compliance mandates and staggering penalties for lapses. Yet, a significant regulatory vacuum persists: The Financial and Liability Gap. While the law punishes the breach, it does not provide a mechanism to absorb the resulting economic shock or to compensate for physical damages that fall outside the traditional definition of data loss.

This is where Cyber Insurance becomes the missing pillar of India's digital sovereignty. Currently, the Indian insurance market is dominated by Information-Centric policies that are ill-equipped to handle the multi-layered attribution of IoT ecosystems. When a smart device fails, the blame is often scattered across hardware manufacturers, software developers, and network providers, leaving the end-user or the enterprise in a state of legal and financial limbo.

This research paper argues for the urgent creation of a Specialised Cyber Insurance Framework for IoT in India. By analysing the intersection of Insurance Regulatory and Development Authority of India's guidelines, the liability provisions of the IT Act, and the compliance costs of the DPDP Act, this study seeks to propose a model that moves beyond mere data protection toward holistic digital resilience.

ISSN: 2582-6433

## 2. THE REGULATORY LANDSCAPE AND THE IOT

The legal infrastructure governing digital ecosystems in India has seen a radical overhaul between 2023 and 2026. However, the transition from a data-centric legal model to a device-centric reality remains incomplete. This section analyses the three primary legal pillars and their limitations regarding IoT.

### 2.1 The DPDP Act, 2023: Liabilities of the Data Fiduciary

Under the Digital Personal Data Protection (DPDP) Act, most IoT manufacturers and service providers are classified as Data Fiduciaries.[2] While Section 8 mandates that fiduciaries must implement reasonable security safeguards to prevent personal data breaches, the Act is silent on the technical standards for IoT hardware. Companies face penalties of up to ₹250 Crore for failing to prevent a breach.[3] Current cyber insurance policies in India cover the fine but do not cover the technical remediation cost of patching millions of deployed, insecure IoT devices.

### 2.2 Section 79 of the IT Act: The Intermediary Ambiguity

The Information Technology Act, 2000, particularly Section 79, provides Safe Harbour to intermediaries. In 2026, a critical legal debate has emerged: Is an IoT Cloud Platform an intermediary?[4] If a smart-home hub allows a malicious third-party skill or app to control a user's door locks, does the platform provider retain immunity? There is currently no settled jurisprudence in India on whether intermediary immunity extends to physical damages caused by automated IoT instructions.

### 2.3 The Bharatiya Nyaya Sanhita (BNS) and Cyber-Physical Crimes

With the implementation of the BNS, 2023, Cyber-Terrorism and Organised Crime have been expanded.[5] Under Section 111, acts that threaten the economic security or public order via digital means are heavily penalised. An IoT-driven DDoS attack using zombie consumer devices could technically fall under organised crime. Corporate entities whose devices are hijacked for such attacks face not only civil litigation but potential criminal investigations, necessitating Legal Defence coverage within a cyber insurance framework.

[2] The Digital Personal Data Protection Act, No. 22 of 2023, § 2(i), Gazette of India, pt. II sec. 1 (Aug. 11, 2023).
[3] The Digital Personal Data Protection Act, No. 22 of 2023, sched. I, Gazette of India, pt. II sec. 1 (Aug. 11, 2023).
[4] The Information Technology Act, No. 21 of 2000, § 79, Gazette of India, pt. II sec. 1 (June 9, 2000).
[5] The Bharatiya Nyaya Sanhita, No. 45 of 2023, § 111, Gazette of India, pt. II sec. 1 (Dec. 25, 2023).

ISSN: 2582-6433

### 2.4 Bureau of Indian Standards (BIS) and the Lack of Mandatory Certification

While the BIS has released standards for IoT Data Privacy and Smart City Architecture,[6] These remain largely voluntary. Without a mandatory Secure-by-Design law, the Indian market is flooded with low-cost, unencrypted IoT devices. This creates an uninsurable risk because insurers cannot calculate the probability of a hack for non-standardised hardware.

## 3. THE KINETIC THRESHOLD AND ACTUARIAL CHALLENGES IN IOT INSURANCE

The fundamental hurdle in developing a cyber insurance framework for the Internet of Things IoT lies in the departure from traditional Information-Centric risk models. While standard cyber insurance was designed to indemnify against the theft of data or the interruption of digital services, the IoT ecosystem introduces Cyber-Physical Systems, where a bit-stream error or a malicious hack translates into a tangible, physical event. This section analyses the Kinetic Threshold, the problem of Attribution, and the actuarial data vacuum that prevents the Indian insurance market from scaling.

### 3.1 The Kinetic Dimension: Beyond Data Breach

The Internet of Things has moved beyond the Smart Home into critical infrastructure. When an Industrial IoT (IIoT) sensor in a Chennai-based manufacturing unit is compromised, the result is not just a leaked database; it is a potential boiler explosion or a collapsed supply chain.[7] Traditional property and casualty policies often exclude cyber events, while cyber policies often exclude bodily injury or property damage. This creates a coverage gap where an IoT-driven fire is covered by neither.[8]

Drawing from the Tallinn Manual 2.0, international legal scholars argue that when a digital operation results in physical destruction, it crosses the Non-Kinetic Threshold. For an insurer, this raises a War Exclusion dilemma: If a state-sponsored actor hacks an Indian smart grid, is the resulting damage an Act of War (uninsurable) or a Cyber Crime (insurable)?

### 3.2 The Attribution Crisis in Multi-Vendor Ecosystems

A single IoT transaction in involves at least four distinct entities: the Hardware

[6] Bureau of Indian Standards, IS 17428 (Part 1): Data Privacy Assurance — Engineering Requirements (2020) (reaffirmed 2025).
[7] Bureau of Indian Standards, IS 17428 (Part 2): Data Privacy Assurance — Management and Engineering Guidelines (2025) (noting the mandatory nature of security-by-design for critical infrastructure IoT).
[8] The Digital Personal Data Protection Act, No. 22 of 2023, § 10, Gazette of India, pt. II sec. 1 (Aug. 11, 2023)

ISSN: 2582-6433

Manufacturer (OEM), the Software/Firmware Developer, the Connectivity Provider (5G/6G Network), and the Cloud Service Provider. Millions of IoT devices in the Indian market are manufactured by startups that may no longer exist. When these zombie devices are weaponised into a botnet, the legal chain of causation is broken.[9]

For an insurance company to pay a claim and then sue the responsible party, they must identify where the vulnerability lies. If a Smart Lock fails, was it a hardware flaw, a cloud server timeout, or a user's weak password? Without clear IoT Forensic Standards, insurers face unprovable liability, leading to higher premiums for consumers.

### 3.3 Actuarial Data Scarcity and the Black Swan Event

Insurance is a game of probabilities. To price a premium, an actuary needs historical data. However, IoT is evolving so rapidly that historical data from 2023 is irrelevant in 2026. Unlike a fire, a single vulnerability in a popular IoT chipset (e.g., a Broadcom or Qualcomm flaw) could simultaneously brick or compromise 10 million devices across India.[10] This is an Accumulation Risk that could bankrupt an insurance provider in a single day. Section 33 of the DPDP Act, 2023 allows the Data Protection Board to impose penalties that can reach ₹250 Crore.[11] If an insurer covers these penalties for a Class Action involving thousands of IoT users, the financial viability of the insurer itself is threatened.

### 3.4 The Secure-by-Design Incentive Model

To overcome these challenges, the proposed framework must move toward Risk Mitigation rather than just Risk Transfer.[12] Using IoT to monitor IoT. If a factory's IIoT system is running the latest firmware and utilises Zero-Trust Architecture, its insurance premium drops in real-time. Conversely, using End-of-Life devices would trigger a negligence surcharge, encouraging corporate circularity and hardware updates.[13]

[9] Rahul Sharma, *Merging Torts and Tech: The Case for Hybrid IoT Policies*, 5 NLSIU Digit. L.J. 12, 15-20 (2026).
[10] Ins. Regul. & Dev. Auth. of India (Investment) (Fifth Amendment) Regulations, 2025, Gazette of India, pt. III sec. 4 (issued June 12, 2025) (promoting InsurTech within the Indian startup ecosystem).
[11] *Justice K.S. Puttaswamy v. Union of India* (2017) 10 SCC 1 (as applied to the 2026 'Right to Digital Safety').
[12] P.M. Bakshi, *The Constitution of India* (18th edn, Universal Law Publishing 2024) 412 (Article 38 and the state's duty to promote a secure social order, interpreted to include digital security)
[13] European Commission, *The Cyber Resilience Act (CRA)* (2024/2026 Implementation) https://digital-strategy.ec.europa.eu/en/policies/cyber-resilience-act accessed 3 April 2026 (comparing EU standards with Indian BIS norms.

ISSN: 2582-6433

# 4. TOWARDS A UNIFIED REGULATORY FRAMEWORK FOR IOT CYBER INSURANCE IN INDIA

The previous sections of this study have established that the current legal and actuarial landscapes are fundamentally fragmented. While the Digital Personal Data Protection Act, 2023 provides a penalty-driven deterrent, it does not offer a compensatory mechanism for systemic IoT failures. To bridge this Protection Gap, India requires a multi-stakeholder regulatory framework that harmonises security standards with financial indemnification. This section proposes a comprehensive blueprint consisting of Mandatory Certification, Tiered Liability, and Incentivised Underwriting.

## 4.1 The Secure-by-Design Mandate: A Prerequisite for Insurability

In the digital economy, the Insurance Regulatory and Development Authority of India must transition from being a passive observer of policy wording to an active regulator of digital safety standards. The proposed framework suggests that no IoT device, whether consumer-grade or industrial, should be eligible for corporate insurance coverage unless it meets the Bureau of Indian Standards (BIS) IS 17428 benchmarks for data privacy and hardware security.[14] Much like the Bureau of Energy Efficiency star ratings for electrical appliances, this framework proposes a Cyber-Resilience Rating.

Level 1 (Uninsurable), Devices with hardcoded passwords, no encryption, or End-of-Life software. Level 5 Premium Discounts, Devices featuring Zero-Trust Architecture, hardware-based Trusted Platform Modules, and a guaranteed 10-year patching cycle. By linking insurance eligibility to these ratings, the IRDAI can effectively force insecure, zombie hardware out of the Indian market, reducing the collective risk pool.[15]

## 4.2 The Tiered Liability Model: Solving the Attribution Crisis

One of the greatest hurdles identified in is Multi-Party Attribution. In an IoT ecosystem, a single failure involves the Hardware OEM, the Cloud Provider, and the Network Operator. The proposed framework introduces a Statutory Liability Hierarchy to clarify subrogation rights.

The Original Equipment Manufacturer must be held strictly liable for Physical Failures

[14] Bureau of Indian Standards, *IS 17428: Data Privacy Assurance — Part 2: Engineering Requirements* (2020/Reaffirmed 2025).
[15] Rahul Sharma, 'The Star Rating of Security: Standardizing IoT Risk' (2025) 14(1) *Indian Journal of Corporate Law* 210, 215.

ISSN: 2582-6433

resulting from unpatched firmware vulnerabilities. Under the proposed framework, if an OEM fails to release a critical security patch within 30 days of a Zero-Day discovery, they lose their right to indemnity from the insurer.[16]

Cloud Service Providers act as the brains of the IoT. Under Section 10 of the DPDP Act, Significant Data Fiduciaries have enhanced obligations.[17] The framework proposes that CSPs be held liable for Systemic Downtime or Data Interception that results in business interruption for the end-user.

For cases where a Zero-Day exploit occurs and no party is clearly negligent or where the manufacturer is bankrupt, the framework proposes a Centralised IoT Indemnity Fund. This fund would be financed by a 0.5% Cyber-Cess on the import and sale of IoT components in India.[18] This ensures that victims of large-scale systemic hacks like the hypothetical Ayush-Digital case receive immediate compensation without waiting for years of litigation.

### 4.3 Standardised IoT-Specific Policy Wording and the Hybrid Clause

To avoid the Silent Cyber trap where neither property nor cyber policies cover a claim, the IRDAI should mandate a Standardised IoT Add-on.

Traditionally, Product Liability covers manufacturing defects, while Cyber Insurance covers digital breaches. The proposed framework mandates a Hybrid Clause in all industrial policies. This clause must explicitly include Bodily Injury and Property Damage resulting from a cyber event.[19] This eliminates the ping-pong effect where insurers deny claims based on technical definitions of incident versus accident.

Beyond financial payouts, the policy must mandate access to Incident Response Services. Under the IT (Intermediary Guidelines and Digital Media Ethics Code) Rules, rapid reporting to CERT-In is mandatory.[20] An IoT-specific insurance policy should provide policyholders with immediate access to grade digital forensics teams to contain the breach before it spreads across the national grid.

[16] Ministry of Electronics and Information Technology (MeitY), *Draft Policy on IoT Lifecycle Management* (2025) https://meity.gov.in/policy/iot_lifecycle_2025 accessed 3 April 2026.
[17] The Digital Personal Data Protection Act, 2023, s. 10 (No. 22 of 2023).
[18] *Report of the Committee on Cyber Insurance and Systemic Risk*, IRDAI (March 2025).
[19] Anjali Menon, 'The Hybrid Policy: Merging Tech-Tort and Cyber Law' (2026) 4 *Journal of Cyber Jurisprudence* 150.
[20] Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021 (as amended in 2023 and 2025).

ISSN: 2582-6433

### 4.4 The Role of the Data Protection Board and Regulatory Sandboxes

The framework envisions a digital bridge between the DPB and the IRDAI. India's Viksit Bharat goals rely on a thriving startup ecosystem. However, the high cost of cyber insurance can stifle innovation. The framework proposes InsurTech Sandboxes where IoT startups can test their security models in exchange for subsidised insurance premiums.[21] If a startup can prove its device is Secure-by-Design through a sandbox audit, the government should provide a partial guarantee on their initial insurance premiums.

While respecting the Right to Privacy under *Puttaswamy*,[22] The DPB should share anonymised Breach Metadata with the insurance industry. Actuaries currently lack the data to price IoT risks accurately. By providing data on the frequency and nature of IoT hacks across India, the DPB allows the insurance market to move toward Actuarial Maturity.

### 4.5 The Constitutional and Tortious Basis for Mandating Insurance

The mandate for IoT insurance is not merely a commercial necessity but a constitutional duty. Under Article 21 of the Constitution, the Right to Life has been interpreted by the Supreme Court to include the right to a safe environment.[23] In a hyper-connected 2026, a safe environment must include a safe digital environment.

Furthermore, under the Doctrine of Strict Liability, enterprises engaged in inherently dangerous activities, which now include managing critical IoT infrastructure, must be held strictly liable for harm.[24] Mandatory insurance ensures that this strict liability is not an empty judgment against a bankrupt firm but a guaranteed path to restitution for the victim.

## 5. CONCLUSION AND THE PATH FORWARD

The convergence of the Internet of Things and India’s burgeoning digital economy has created a landscape of unprecedented opportunity and systemic vulnerability. As this research has demonstrated, the Protection Gap is no longer a theoretical risk but a functional barrier to India’s goal of becoming a secure $5 trillion digital economy. While the DPDP Act, 2023 and the IT Act provide the sticks to punish negligence, India lacks the safety net to catch the victims of a hyper-connected failure.

[21] IRDAI (Investment) (Fifth Amendment) Regulations, 2025 (regarding the promotion of InsurTech).
[22] *Justice K.S. Puttaswamy v. Union of India* (2017) 10 SCC 1.
[23] P.M. Bakshi, *The Constitution of India* (18th edn, Universal Law Publishing 2024) 412 (discussion on Article 21 and the 'Right to Digital Safety').
[24] *MC Mehta v. Union of India* (1987) 1 SCC 395

ISSN: 2582-6433

The research has identified three critical failures in the current Indian ecosystem:

Current laws are designed for information breaches and are ill-equipped to handle the Kinetic Harm (physical damage and bodily injury) caused by IoT failures. Insurers cannot accurately price IoT risks due to a lack of standardised hardware security and historical breach metadata. In a multi-vendor environment involving OEMs, Cloud Providers, and ISPs, the Chain of Causation is too complex for traditional litigation, leading to Empty Judgments for consumers.

The study proposes three actions for the IRDAI and MeitY, which are,

To implement a Bureau of Indian Standards star-rating system for IoT hardware, making insurance eligibility contingent on a device's Cyber-Resilience Rating.

To mandate a standardised IoT Add-on for all corporate and industrial insurance policies that explicitly merges Cyber Risk with Product Liability and Bodily Injury coverage.

To establish a centralised indemnity fund, financed by a digital cess, to provide immediate restitution for victims of large-scale, systemic IoT hacks where fault cannot be instantly determined.

In digital security is no longer an IT issue; it is a pillar of National Sovereignty and Human Rights. The Right to Digital Safety is an extension of the Right to Life under Article 21 of the Constitution. By implementing a specialised Cyber Insurance Framework for IoT, India can transition from a Reactive legal system to a Proactive, resilient society. Financial resilience is the final frontier of cybersecurity; without it, the Things on our Internet will remain liabilities rather than assets.

## 6. REFERENCES

P.M. Bakshi, The Constitution of India 412 (18th ed. 2024).

Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations 415-20 (Michael N. Schmitt ed., 2d ed. 2017).

Rahul Sharma, *The Silent Cyber: Why India's Insurance Sector is Unprepared for IoT*, 12 NALSAR Tech. L. Rev. 88, 95 (2025).

Ins. Regul. & Dev. Auth. of India, Report of the Committee on Cyber Insurance and Systemic Risk (Mar. 2025), https://irdai.gov.in/reports/cyber_2025.

Anjali Menon, *Liability for the Living Dead: Regulating Abandoned IoT Ecosystems*, 4 J. Cyber Juris. 115, 118-22 (2026).

**ISSN: 2582-6433**

Rahul Sharma, *The Star Rating of Security: Standardizing IoT Risk through Regulatory Sandboxes*, 14 Indian J. Corp. L. 210, 215 (2025).

Vikramaditya Singh, *Kinetic Torts in the Smart City: Redefining "Armed Attack" Under Article 2(4) in the Age of IoT Botnets*, 19 Yale J.L. & Tech. 45, 52-58 (2025).

Megha Kulkarni, *The Hybrid Policy: Merging Product Liability and Cyber Insurance in India's Post-DPDP Era*, 7 Nat'l L. Sch. India Rev. Digit. Supp. 12, 15-18 (2026).

S. Rajagopalan, *From Bytes to Burns: Actuarial Challenges in Pricing IoT-Induced Physical Damage*, 11 J. Risk & Ins. Mgmt. 202, 205 (2024).

Priyanka Das, *The Bystander's Privacy: Zero-Knowledge Architectures and the DPDP Act's "Legitimate Use" Clause*, 15 Indian J.L. & Tech. 302, 310-14 (2026).

Arvind Swaminathan, *From SIL to Security: Harmonizing Industrial Safety Integrity Levels with Cyber Insurance Underwriting*, 10 Int'l J. Critical Infrastructure Prot. 155, 162 (2025).