International Journal of Computer Information Systems and Industrial Management Applications
ISSN 2150-7988 Volume 18(14s) 2026 pp. 416-437
https://doi.org/10.70917/ijcisim-2026-4240
Article

AI and Critical Infrastructure Protection in India: Legal Gaps and Regulatory Reform - Lessons from the EU

Kavita Ajay Joshi[1a, b], Shikha Dimri[2], Lalit Singh[3a, b], Vishesh Yadav[4]

[1a]Department of PDP, Graphic Era Hill University, Bhimtal, Uttarakhand, India.
[1b] Centre for Promotion of Research, Graphic Era Deemed to be University, Dehradun, Uttarakhand – 248002, India.
Email: kajoshi@gehu.ac.in
ORCID: 0000-0003-3842-8080
[2]School of Law, UPES, Dehradun, Uttarakhand, India.
Email: shikha@ddn.upes.ac.in
ORCID: 0000-0002-2973-3131
[3a]Department of PDP, Graphic Era Hill University, Bhimtal, Uttarakhand, India.
[3b] Centre for Promotion of Research, Graphic Era Deemed to be University, Dehradun, Uttarakhand – 248002, India.
Email: lalitsingh.btl@gehu.ac.in
ORCID: 0000-0001-6432-3616
[4] High Court of Judicature at Allahabad, Lucknow Bench; Department of Law, Amity Law School, Amity University, Lucknow, Uttar Pradesh, India.
Email: visheshchandra17@gmail.com
ORCID: 0009-0002-9404-4743

Abstract: India's Critical Information Infrastructure (CII) has been subjected to a series of high-profile cyber-attacks that have collectively exposed fundamental legal, regulatory, and systemic gaps within its protection framework-gaps that are being dangerously amplified by the accelerating and institutionally fragmented deployment of Artificial Intelligence (AI) across critical sectors. The 2019 Kudankulam Nuclear Power Plant (KKNPP) Dtrack malware intrusion revealed a complete accountability vacuum regarding third-party contractors operating within nuclear-critical IT networks. The 2022 AIIMS New Delhi ransomware attack paralysed India's premier healthcare institution for fifteen days, exposing the absence of mandatory network micro-segmentation and ex-ante penetration testing requirements. The 2020 Mumbai power grid collapse, linked to the Chinese state-sponsored RedEcho group's ShadowPad malware campaign, demonstrated how Indian law treats energy-sector cybersecurity as a static compliance checklist while ignoring the algorithmic manipulation of automated load-balancing systems. The 2023 CoWIN data leak, involving automated API scraping of vaccination records of millions of citizens, revealed the absence of any Data Protection by Design mandate in public-utility software architectures. Compounding these sector-specific failures is a deeper structural pathology: AI governance in India is not regulated by a single, statutory authority but by a mosaic of at least eleven distinct bodies, each with overlapping, uncoordinated, and non-binding jurisdiction to govern AI, with no single statutory body having any overarching rule-making or enforcement authority. This paper assesses these gaps using a doctrinal and comparative legal approach, by comparing the Indian regulatory framework with the harmonised legal framework of the European Union (EU) consisting of the NIS 2 Directive, the EU AI Act and the GDPR. The paper outlines a blueprint for legislative change that can be achieved over five pillars: a Tiered AI-Risk Classification Model for Indian CII, a requirement for cyber-auditing obligations in supply chains, a requirement for human-in-the-loop kill-switches, Data Protection by Design requirements, and a statutory coordinating authority for AI-CII responsibilities, directly following the diagnosis in the mosaic-model approach to AI-CII oversight. The analysis highlights that India's sectoral, reactive, fragmented and notification-dependent approach is structurally

weak to tackle the AI-specific threat landscape and recommends for an inter-sectoral, proactive, risk-proportionate legislative reform which can pre-emptively address the threat landscape of AI

Keywords: Critical Information Infrastructure; Artificial Intelligence Regulation; EU AI Act; Cybersecurity Governance; Information Technology Act;

1. Introduction

AI and CII protection is one of the most impactful regulatory challenges facing nation states in the 21st century. Governments are making increasingly more use of AI-powered systems in their energy grid, healthcare networks, nuclear facilities and public utility digital platforms, resulting in the attack surface being increased in a way that legacy cyber security systems were never built to deal with[footnoteRef:1]. India is home to over 900 million internet users, the most populous country as well as a rapidly digitalising economy, making the challenge even more acute in India. The Information Technology Act, 2000 (IT Act) – India's main and fundamental cyber-law framework was passed before the advent of machine learning systems for automatic decision making, the weaponisation of software supply chains as advanced cyber attack vectors, and the introduction of AI hallucinations as a systemic threat on regulatory and even judicial integrity.[footnoteRef:2].

The urgency of this inquiry is demonstrated by four landmark cyber-incidents that together expose the full spectrum of India's regulatory deficiencies across the nuclear, healthcare, energy, and digital-public-service sectors. First, the 2019 Kudankulam Nuclear Power Plant (KKNPP) Dtrack malware intrusion, attributed to the North Korean state-sponsored Lazarus Group, revealed a fundamental accountability vacuum regarding third-party vendors and contractors operating within nuclear-critical IT networks-a gap wholly unaddressed by Section 70 of the IT Act[footnoteRef:3]. Second, the 2022 AIIMS New Delhi ransomware attack, reportedly perpetrated by the LockBit gang, paralysed one of India's premier healthcare institutions for over fifteen days and exposed the complete absence of any statutory requirement for mandatory network micro-segmentation, regular penetration testing, or proactive vulnerability assessment under Indian law[footnoteRef:4]. Third, the 2020 Mumbai power grid collapse, temporally coincident with the India-China Ladakh standoff and linked by Recorded Future's Insikt Group to the Chinese state-sponsored RedEcho group's ShadowPad malware campaign, demonstrated how Indian energy-sector cybersecurity law treats grid protection as a static checklist of conventional IT controls, wholly ignoring the specific and novel risk of algorithmic manipulation of AI-driven automated load-balancing and dispatch systems[footnoteRef:5]. Fourth, the 2023 CoWIN data leak, wherein personally identifiable data-including Aadhaar numbers, PAN card numbers, passport details, and vaccination records-of millions of Indian citizens was scraped via automated exploitation of inadequately protected API endpoints, revealed the absence of any statutory "Data Protection by Design" mandate governing the architectural security of public-utility digital platforms[footnoteRef:6].

In marked contrast to India's fragmented, reactive, and largely advisory regulatory posture, the European Union has systematically constructed a harmonised, interlocking, and legally binding regulatory architecture consisting of three principal instruments. The NIS 2 Directive (Directive (EU) 2022/2555), which entered into force on 16 January 2023, mandates comprehensive cybersecurity risk-management measures-including, critically, supply-chain security auditing under Article 21(2)(d)-for essential and important entities across eighteen designated sectors, with enforcement backed by administrative fines of up to €10 million or 2% of worldwide annual turnover[footnoteRef:7]. The EU AI Act (Regulation (EU) 2024/1689), the world's first comprehensive AI-specific legislation, classifies AI systems deployed in critical infrastructure as "high-risk" under Article 6, read with Annex III, and imposes mandatory human oversight (Article 14), and accuracy, robustness, and cybersecurity requirements (Article 15)[footnoteRef:8]. The General Data Protection Regulation (GDPR, Regulation (EU) 2016/679), whose Article 25 imposes a binding "Data Protection by Design and by Default" obligation on all data controllers and processors, completes the triad[footnoteRef:9].

This paper is further contextualised by two contemporaneous developments. First, the National Crime Records Bureau's (NCRB) latest published statistics, as reported in the Ministry of Home Affairs' Press Information Bureau release dated 21 July 2026, reveal that total registered cyber crimes in India have more than doubled from 50,035 in 2020 to 101,928 in 2024-a compound annual growth rate (CAGR) of approximately 19.5%-with cyber fraud cases alone tripling from 10,395 to 29,758 over the same period[footnoteRef:10]. Second, the Supreme Court of India's landmark judgment in Pooja Ramesh Singh v. Jammu and Kashmir Bank Ltd. (2026 INSC 668), delivered on 2 July 2026, set aside judgments of the NCLT and NCLAT after discovering that the adjudicating tribunal had relied on "non-existent, fake and hallucinated material, generated through Artificial Intelligence, as if it were a precedent in support of its judgment," and declared "zero tolerance" for the citation of unverified AI-generated legal

material[footnoteRef:11]. The decision is a testament to the key finding of this paper: India's current laws are fundamentally ill-equipped for the age of artificial intelligence in all aspects of governance. .

That India is unprepared is not just a doctrinal issue; it is an institutional matter as well. As Section 3.2 of this paper illustrates, India does not have a single competent regulatory body for AI, but rather, multiple ministries, standard bodies and sectoral regulators, none of whom have a centralised statutory jurisdiction. This paper argues that this institutional fragmentation is a serious legal gap distinct from the four substantive gaps revealed by the case studies, and one which needs to be resolved in conjunction with these

This paper is organized as follows. Section 2 outlines the research methodology, and provides a scope note that is explicit to differentiate AI-direct from AI-adjacent case evidence. Section 3 provides a detailed comparative legal framework analysis of Indian and EU instruments, including an examination of India's fragmented multi-agency AI regulatory mosaic. Section 4 presents four forensic case studies with granular legal-gap mapping, supported by quantitative data visualisations. Section 5 proposes a comprehensive five-pillar legislative reform blueprint. Section 6 presents conclusions.

2. Research Methodology

This paper employs a doctrinal and comparative legal research methodology, supplemented by empirical case-study analysis and contextualised by quantitative cybercrime data. The doctrinal component involves a systematic examination of primary legal sources including statutes, delegated legislation, regulatory directives, implementing regulations, and judicial pronouncements across two jurisdictions.

The Indian statutory corpus examined includes: (i) the Information Technology Act, 2000 (as amended in 2008), particularly Sections 43, 43A, 66, 66F, 69, 70, 70A, 70B, and 79; (ii) the Information Technology (Information Security Practices and Procedures for Protected System) Rules, 2018; (iii) the Information Technology (National Critical Information Infrastructure Protection Centre and Manner of Performing Functions and Duties) Rules, 2013; (iv) the CERT-In Directions of 28 April 2022; (v) the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Amendment Rules, 2026, notified 10 February 2026[footnoteRef:12]; (vi) the Digital Personal Data Protection Act, 2023, and the DPDP Rules, 2025; (vii) the Central Electricity Authority Cyber Security in Power Sector Guidelines, 2021; and (viii) NCIIPC Guidelines for the Protection of National Critical Information Infrastructure.

The EU corpus examined includes: (i) the NIS 2 Directive (Directive (EU) 2022/2555); (ii) Commission Implementing Regulation (EU) 2024/2690; (iii) the EU AI Act (Regulation (EU) 2024/1689); (iv) the GDPR (Regulation (EU) 2016/679); and (v) the Critical Entities Resilience Directive (Directive (EU) 2022/2557). Comparative methodology identifies the similarities and differences between similar obligations in the Indian constitutional structure and the EU framework, not only in words but in the structure of the law.

2.1 Scope Note: AI-Direct and AI-Adjacent Case Evidence

The methodological nature of the four case studies analyzed in Section 4 is certain, which brings up a clarification of the evidentiary nature of the case studies. The Mumbai power grid incident (Case 3) is analysed as an AI-direct case: the specific legal gap identified-the absence of a human-in-the-loop safeguard-concerns the actual or prospective algorithmic control of load-dispatch decisions by automated systems. The Kudankulam (Case 1), AIIMS (Case 2), and CoWIN (Case 4) incidents, by contrast, are analysed as AI-adjacent extension cases: each was, in its own historical occurrence, a conventional malware, ransomware, or data-scraping incident rather than a failure of an AI system per se. This paper's analytical method treats these three incidents as diagnostic of the underlying legal architecture-the absence of supply-chain auditing, network segmentation, and Data Protection by Design-that would apply with equal or greater force were an AI system layered onto the same infrastructure, as is now occurring across Indian healthcare, nuclear, and public-digital-service sectors under the IndiaAI Mission and allied initiatives. This distinction is made explicit here so that the reader may evaluate the strength of the inference in each case on its own terms: the AI-direct case (Mumbai) demonstrates a live AI-specific regulatory gap, while the AI-adjacent cases (KKNPP, AIIMS, CoWIN) demonstrate the structural preconditions-vendor accountability, architectural resilience, and design-stage privacy-without which any subsequent AI deployment in those sectors would inherit the same vulnerabilities.

Quantitative cybercrime data is sourced from the NCRB "Crime in India" publication series (2020-2024) and the I4C-operated CFCFRMS and NCRP platforms, as reported in the PIB release of 21 July 2026[footnoteRef:13]. This data is visualised in Figures 2-4 to support the argument in Section 4.5. The four case studies are selected on the

basis of sectoral representativeness-nuclear, healthcare, energy, and digital public services-and the availability of verified public-domain forensic accounts from government agencies, cybersecurity firms (Recorded Future, Kaspersky, Issue Makers Lab), judicial records, and investigative journalism.

3. Comparative Legal Framework Analysis

3.1 India's CII Protection Architecture: Structural Overview

India's CII protection framework is anchored in three principal statutory pillars within the Information Technology Act, 2000. Section 70 empowers the "appropriate Government" to declare any computer resource whose incapacitation or destruction would have a "debilitating impact on national security, economy, public health or safety" as a "Protected System." Once so notified, the appropriate authority authorises specified persons to access the system, and unauthorised access attracts imprisonment up to ten years and a fine under Section 70(3)[footnoteRef:14]. Section 70A (inserted via the 2008 Amendment) establishes the National Critical Information Infrastructure Protection Centre (NCIIPC), operating under the administrative control of the National Technical Research Organisation (NTRO), as the national nodal agency for CII protection[footnoteRef:15]. Section 70B designates the Indian Computer Emergency Response Team (CERT-In) as the nodal agency for cybersecurity incident response, empowered to collect, analyse, and disseminate information on cyber incidents and to issue binding directions[footnoteRef:16].

The NCIIPC has identified six critical sectors for CII protection: (i) Power and Energy; (ii) Banking, Financial Services and Insurance; (iii) Telecom; (iv) Transport; (v) Government; and (vi) Strategic and Public Enterprises[footnoteRef:17]. The operational compliance framework is provided by the Information Technology (Information Security Practices and Procedures for Protected System) Rules, 2018. In April 2022, CERT-In issued landmark Directions mandating, inter alia, a six-hour incident-reporting window for all entities, mandatory maintenance of logs for 180 days, and time-server synchronisation[footnoteRef:18]. Most recently, the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Amendment Rules, 2026, notified on 10 February 2026 and effective from 20 February 2026, marked a significant shift toward regulating AI-generated and synthetic content, tightening safe-harbour protection under Section 79 and introducing a mandatory three-hour takedown window for flagged content-the first instance of India directly legislating on AI-generated material, albeit confined to content moderation rather than AI-system safety[footnoteRef:19].

Despite these measures, the Indian framework suffers from three fundamental structural deficiencies that this paper identifies as "first-order gaps"-deficiencies not at the level of implementation but at the level of legislative architecture. The first is notification dependent: a computer resource is only "critical" if the Government has "affirmatively and individually" declared it to be, establishing a binary standard where large networks of interconnected computers are vulnerable until the act catches up with technology. Second, the framework is entirely silent on AI-specific risks: no provision of the IT Act, the DPDP Act, or any subordinate regulation addresses the deployment of automated decision-making systems within CII. Third, the framework contains no mandatory supply-chain security obligations.

3.2 India's Fragmented AI Regulatory Mosaic: The Multi-Agency Problem

Beyond the three doctrinal gaps identified in Section 3.1, this paper identifies a fourth, structurally prior deficiency: India does not possess a single, centralised statutory authority responsible for AI governance. Instead, as Figure 1 illustrates, AI regulation in India operates through what this paper terms a "multi-agency mosaic model," in which responsibility is distributed across four functional clusters and at least eleven distinct bodies, none of which possesses comprehensive, binding, cross-sectoral rule-making authority over AI systems.

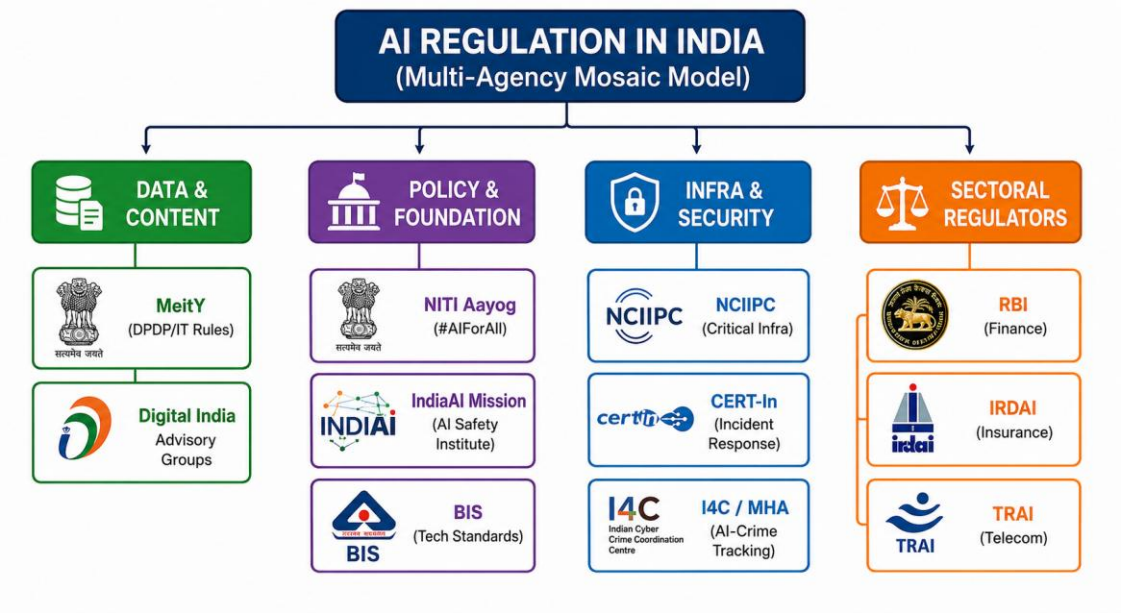

Figure 1. AI Regulation in India: The Multi-Agency Mosaic Model.

Source: Compiled diagrammatic representation of India's AI-governance ecosystem, based on MeitY, NITI Aayog, and IndiaAI Mission institutional mandates as of July 2026.

The first cluster, Data and Content, is occupied by the Ministry of Electronics and Information Technology (MeitY), which administers both the DPDP Act and the IT Rules, and by the Digital India Advisory Groups, which provide non-binding stakeholder input on platform governance. The second cluster, Policy and Foundation, comprises NITI Aayog, whose 2018 National Strategy for Artificial Intelligence articulated the "#AIforAll" vision and whose 2021 two-part approach paper on "Responsible AI" established non-binding ethical principles[footnoteRef:20]; the IndiaAI Mission, approved by the Union Cabinet on 7 March 2024 with a five-year outlay of INR 10,371.92 crore and administratively housed within MeitY, which funds compute infrastructure, indigenous foundation models, and safe-AI research but exercises no regulatory or enforcement function[footnoteRef:21]; and the Bureau of Indian Standards (BIS), which is tasked with developing technical standards for AI risk taxonomies and certification but has yet to publish binding AI-specific standards enforceable against critical-infrastructure operators.

The third cluster, Infrastructure and Security, comprises NCIIPC (critical infrastructure protection under IT Act Section 70A), CERT-In (incident response under Section 70B), and the Indian Cyber Crime Coordination Centre (I4C) under the Ministry of Home Affairs, which tracks AI-enabled crime through the Samanvaya platform and the National Cyber Crime Reporting Portal[footnoteRef:22]. The fourth cluster, Sectoral Regulators, comprises the Reserve Bank of India (RBI) for AI deployed in financial services, the Insurance Regulatory and Development Authority of India (IRDAI) for insurance-sector AI, and the Telecom Regulatory Authority of India (TRAI) for telecommunications AI-each issuing sector-specific guidance without cross-referencing the others' standards or NCIIPC's CII designations.

Critically, MeitY's own recently unveiled India AI Governance Guidelines, published under the IndiaAI Mission, implicitly concede the fragmentation problem: the Guidelines propose the creation of a new "AI Governance Group" as a "high-level body" for "overall policy formulation and coordination of AI governance in India across all agencies," explicitly acknowledging that government agencies (MeitY, the Ministry of Home Affairs), sectoral regulators (RBI, SEBI, TRAI, the Competition Commission of India), advisory bodies (NITI Aayog, the Office of the Principal Scientific Adviser), and standards bodies (BIS, the Telecommunication Engineering Centre) currently operate without such coordination[footnoteRef:23]. However, as of the date of this paper, the proposed AI Governance Group remains a policy recommendation rather than a statutorily constituted body with binding rule-making or enforcement powers. Separately, a private member's bill-the Artificial Intelligence (Ethics and Accountability) Bill, 2025, introduced in the Lok Sabha in December 2025-proposes a statutory AI Ethics Committee with powers to mandate ethical reviews, bias audits, and penalties of up to INR 5 crore, but has not been enacted and does not enjoy Government sponsorship[footnoteRef:24]. The long-anticipated Digital India Act, first announced in 2022 to replace

the IT Act, 2000 in its entirety and expected to introduce risk-based classification of digital platforms including AI systems, remains in draft consultation as of 2026, with no enacted text or firm legislative timeline[footnoteRef:25].

The consequence of this mosaic structure, for the purposes of this paper's argument, is threefold. First, no single body can mandate the tiered AI-risk classification proposed in Section 5.1 across sectors-NCIIPC lacks jurisdiction over AI deployed in insurance or telecom, while IRDAI and TRAI lack jurisdiction over nuclear or energy CII. Second, supply-chain security obligations (Section 5.2) cannot be uniformly imposed, since vendors serving multiple CII sectors would face inconsistent or absent requirements depending on which regulator, if any, asserts jurisdiction. Third, and most importantly, the absence of a central coordinating authority means that even where individual bodies (NCIIPC, CERT-In, sectoral regulators) issue guidance, there is no mechanism to ensure consistency, close jurisdictional gaps, or assign accountability when an AI-enabled CII incident straddles multiple regulatory domains-precisely the scenario witnessed in the Mumbai grid incident, where energy-sector cybersecurity, national-security concerns, and (prospectively) AI-system governance would today fall across CEA, NCIIPC, CERT-In, and no clearly designated AI regulator simultaneously. This diagnosis directly informs Pillar V of the reform blueprint proposed in Section 5.5.

3.3 The EU's Harmonised Regulatory Architecture

The EU's regulatory architecture is distinguished by three characteristics absent from the Indian framework: horizontal harmonisation across Member States, ex-ante risk stratification, and interlocking sectoral coverage creating a "regulatory mesh" in which gaps in one instrument are covered by another. The NIS 2 Directive, replacing the original NIS Directive (2016/1148), entered into force on 16 January 2023 with a transposition deadline of 17 October 2024[footnoteRef:26]. By that deadline, 23 of 27 EU Member States faced infringement procedures for incomplete transposition, reflecting the ambition and complexity of the directive's requirements. NIS 2 substantially broadens sectoral coverage from the original NIS Directive's six sectors to eighteen, and introduces two categories of regulated entities-"essential" and "important"-based on sector, entity size, and societal significance.

Article 21 of NIS 2 establishes ten mandatory cybersecurity risk-management measures that all essential and important entities must implement on an "all-hazards" basis, including policies on risk analysis, incident handling, business continuity, supply-chain security (Art. 21(2)(d)), vulnerability handling, cyber hygiene training, cryptography policies, human-resources security and access control, and multi-factor authentication[footnoteRef:27]. Article 21(2)(d)'s supply-chain security requirement mandates that entities address "security-related aspects concerning the relationships between each entity and its direct suppliers or service providers," effectively creating a legally binding obligation that cascades security requirements down the entire supply chain. Commission Implementing Regulation (EU) 2024/2690, adopted in October 2024, provides granular technical and methodological specifications for implementing these measures[footnoteRef:28].

The EU AI Act, adopted on 13 June 2024 and entering into force on 1 August 2024 with staggered compliance deadlines extending to August 2027, establishes the world's first comprehensive, risk-tiered regulatory framework for AI systems[footnoteRef:29]. The Act classifies AI systems into four risk tiers: unacceptable risk (prohibited-Art. 5), high risk (stringent compliance obligations-Arts. 6-27), limited risk (transparency obligations-Art. 50), and minimal risk. Article 6, read with Annex III, classifies AI systems used as safety components of, or embedded within, critical infrastructure-including digital infrastructure, road traffic, water supply, gas, heating, and electricity systems-as "high-risk." Article 14 mandates that deployers of high-risk AI systems assign human oversight responsibilities to natural persons with authority to "decide, in any particular situation, not to use the high-risk AI system or to otherwise disregard, override or reverse the output." Article 15 imposes specific requirements for accuracy, robustness, and cybersecurity.

The GDPR completes the triad. Article 25 mandates "Data Protection by Design and by Default," requiring data controllers to implement appropriate technical and organisational measures-such as pseudonymisation, data minimisation, and purpose limitation-"both at the time of the determination of the means for processing and at the time of the processing itself"[footnoteRef:30]. Violations attract administrative fines of up to €20 million or 4% of worldwide annual turnover under Article 83(5). Directly, No EU-wide regulator exists, with implementation of the AI Act handed over to market-surveillance bodies across the EU, but where there is one EU-wide entity, it is the EU AI Office, which is given a uniform substantive duty to enforce the EU AI Act, whereas India's regulators implement the Act under completely different statutory powers and duties and do not have any common substantive duties.

Table 1. Comparative Legal Framework: India vs. European Union

Regulatory Dimension	India	European Union
Central AI Authority	None; 11-body mosaic model (Fig. 1)	EU AI Office + national market-surveillance authorities under one Regulation
Primary CII Statute	IT Act 2000, S.70/70A/70B	NIS 2 Directive (EU) 2022/2555
CII Designation Mechanism	Government notification (case-by-case)	Sector-based self-identification + size thresholds
Supply Chain Security	No statutory mandate; NCIIPC advisory only	NIS 2, Art. 21(2)(d); mandatory with penalties
AI-Specific Risk Classification	Absent; no enacted AI-specific legislation	EU AI Act, Art. 6 + Annex III; 4-tier risk model
Human Oversight of AI in CII	Absent	EU AI Act, Art. 14; mandatory HITL for high-risk
Incident Reporting Timeline	CERT-In: 6 hours (2022 Directions)	NIS 2, Art. 23: 24h/72h/1-month tiered
Data Protection by Design	DPDP Act 2023: general duty; no DPbD	GDPR, Art. 25; mandatory DPbD & by Default
Maximum Penalties	IT Act: 10 yrs; DPDP: INR 250 crore	NIS 2: €10M/2%; AI Act: €35M/7%; GDPR: €20M/4%

Source: Compiled by author from primary statutory texts cited in footnotes 7-33.

4. Forensic Case Studies: Four-Vector Analysis

4.1 Case 1: The Kudankulam Nuclear Power Plant (KKNPP) Vendor Leak (2019)

4.1.1 Factual Matrix

In September 2019, India's largest civil nuclear facility-the Kudankulam Nuclear Power Plant (KKNPP) in Tamil Nadu, equipped with two Russian-designed VVER-1000 pressurised water reactors producing over 47.4 billion kWh per year-was subjected to a sophisticated malware intrusion[footnoteRef:31]. The malware, subsequently identified as the Dtrack backdoor Trojan, was attributed to the North Korean state-sponsored Lazarus Group (also designated APT38). The intrusion was first identified on 3 September 2019 by a U.S.-based cybersecurity firm that alerted the National Cyber Coordination Centre, which informed both NPCIL and ISRO on 4 September 2019[footnoteRef:32].

NPCIL initially denied the breach in a press release dated 29 October 2019, characterising reports as "false information." However, within 24 hours, NPCIL's parent body issued a corrective statement confirming that the malware had been identified, conveyed by CERT-In, and that the infected PC was connected to the internet-facing administrative network, "isolated from the critical internal network"[footnoteRef:33]. Analysis by Kaspersky Labs confirmed Dtrack as a backdoor Trojan designed for reconnaissance: keylogging, browser-history retrieval, IP-address harvesting, and complete file-system enumeration on drives C and E-indicating prior knowledge of the target system's architecture[footnoteRef:34]. The attack was launched by two groups of North Korean hackers acting in concert, according to South Korea-based Issue Makers Lab, which said that the entry point was through a spear-phishing email sent to high-level nuclear scientists, including Anil Kakodkar, the former chairman of the Atomic Energy Commission, who specialises in thorium-based reactor technology.[footnoteRef:35]. The assessed motive was to spy on India's advanced thorium-based nuclear power technology, which North Korea is not allowed to legally get a hold of due to the UN sanctions.[footnoteRef:36].

4.1.2 Legal Gap: Third-Party Contractor Accountability Vacuum

The KKNPP incident highlights a basic failure in section 70 of the IT Act, as it designates a system or the systems as a "Protected System" but does not impose any obligation on the supply chain (vendors, contractors, maintenance agencies, and third-party service providers) that maintain the system, service it, upgrade it, and physically access it. As per the existing Indian law, there is no statutory requirement for NPCIL (or any CII operator) to conduct pre-contractual cyber security due diligence on its IT vendors, prescribe binding auditable cyber security clause in procurement contracts, to carry out periodic supply chain risk audit and to make the third party personnel accessing the CII networks undergo background verification in the manner of primary operators.

The NCIIPC Guidelines do cover vendor management, but are not mandatory[footnoteRef:37]. There is no clear and effective statutory definition of designated agencies in the 2018 Protected System Rules, and no clear or effective requirement for third party contractors. There is no clear and effective statutory definition of designated agencies in the 2018 Protected System Rules and no clear and effective requirement for third party contractors.

4.1.3 EU Comparator: NIS 2, Article 21(2)(d) - Mandatory Supply-Chain Auditing

Article 21(2)(d) of NIS 2 is specifically designed to address this issue, requiring measures to be taken in the supply chain, with administrative fines provided under Article 34(4) of up to €10 million or 2% of global annual turnover. Commission Implementing Regulation (EU) 2024/2690 specifies formalised supplier risk-assessment methodologies, contractual security clauses, and incident-notification cascading obligations[footnoteRef:38]. Article 20(2) of NIS 2 further establishes personal accountability for management bodies of essential and important entities. Had an equivalent statutory obligation existed under Indian law, NPCIL would have been legally required to maintain a contractually binding cybersecurity standard for every vendor accessing KKNPP's IT environment.

4.2 Case 2: The AIIMS New Delhi Ransomware Shutdown (2022)

4.2.1 Factual Matrix

On 23 November 2022, AIIMS, New Delhi-managing over 2,500 beds-suffered a catastrophic ransomware attack[footnoteRef:39]. The attack rendered the entire e-Hospital application, hosted by the National Informatics Centre, non-functional, disabling outpatient registration, inpatient admission, laboratory systems, billing, and appointment scheduling[footnoteRef:40]. Five of the hospital's 100 servers (40 physical and 60 virtual) were directly compromised. All hospital services operated manually for over fifteen days, with full restoration confirmed only by 6 December 2022. The attackers-reportedly the LockBit ransomware gang-allegedly demanded approximately INR 200 crore in cryptocurrency[footnoteRef:41]. Approximately 40 million patient records may have been exposed. The Delhi Police's IFSO unit registered a case under Section 66(F) of the IT Act (cyber-terrorism)-the first invocation of this provision for a healthcare ransomware incident[footnoteRef:42].

It was found that AIIMS was using old computers with no network segmentation for a period of about three decades. CERT-In's investigation revealed that two Protonmail accounts have been created in Hong Kong, indicating foreign participation. Shortly after, Indian Council of Medical Research (ICMR) had faced more than 6000 brute force attacks from IP addresses in Hong Kong and successfully fended off the attack thanks to an upgraded firewall, which showed how effective investments in cybersecurity measures can be.

4.2.2 Legal Gap: Absence of Mandatory Micro-Segmentation and Penetration Testing

Two interrelated gaps in the law were discovered during the AIIMS attack. First, Indian law contains no requirement for network micro-segmentation. AIIMS's flat, unsegmented network architecture enabled the ransomware to spread across the entire e-Hospital application. Second, there is no statutory mandate for ex-ante penetration testing of healthcare IT systems. The IT Act's Section 43A references "reasonable security practices" and permits adoption of ISO 27001 standards, but compliance is self-assessed rather than independently audited[footnoteRef:43].

4.2.3 EU Comparator: NIS 2 Essential-Entity Obligations and AI Act Article 15

Under NIS 2, a healthcare institution of AIIMS's scale would qualify as an "essential entity" within the health sector, subject to the complete gamut of Article 21 risk-management measures, including business continuity, vulnerability handling, and cybersecurity-effectiveness assessment. Under the EU AI Act, an AI system deployed within AIIMS's diagnostic or resource-allocation pipeline would be classified as "high-risk" under Annex III, triggering Article 15's accuracy, robustness, and cybersecurity requirements-mandating technical measures functionally equivalent to network segmentation and pre-deployment robustness testing.

4.3 Case 3: The Mumbai Power Grid Collapse (2020)

4.3.1 Factual Matrix

On 12-13 October 2020, Mumbai experienced a massive power outage that halted suburban railway services, shut down the Bombay Stock Exchange temporarily, and affected millions for up to twelve hours[footnoteRef:44]. The outage coincided with the heightened India-China military standoff in Ladakh. In February 2021, Recorded Future's Insikt Group attributed a campaign of cyber-intrusions against twelve Indian critical-infrastructure entities to a Chinese state-sponsored group designated "RedEcho," employing the ShadowPad modular backdoor malware[footnoteRef:45]. Maharashtra's Energy Minister, Nitin Raut, publicly affirmed the cyber-attack link[footnoteRef:46], while the Union Power Minister attributed the outage to "human error," acknowledging cyber-attacks on other grid segments[footnoteRef:47].

Analysis by the U.S. Department of Energy's Idaho National Laboratory CyOTE programme identified 14 unique MITRE ATT&CK® for ICS techniques and 183 observables, confirming access to both IT and OT systems[footnoteRef:48]. In April 2022, Recorded Future reported continued targeting of at least seven State Load Despatch Centres by a related group using ShadowPad via compromised DVR/IP camera devices[footnoteRef:49].

4.3.2 Legal Gap: Static Checklist Approach; No HITL Mandate for AI-Driven Grid Management

The CEA Cyber Security in Power Sector Guidelines, 2021 prescribe traditional technical controls but do not address algorithmic manipulation of AI-driven load-balancing and dispatch systems[footnoteRef:50]. Indian law does not require human oversight of automated load-dispatch decisions, algorithmic transparency, an automated kill switch enabling override of AI-generated dispatch decisions, or robustness testing against adversarial inputs.

4.3.3 EU Comparator: EU AI Act Article 14 - Statutory HITL Kill Switch

An AI system used to manage safety-critical energy decisions would be classified "high-risk" under Annex III, Point 2. Article 14(4) requires that the deployer assign oversight to persons with authority to "decide, in any particular situation, not to use the high-risk AI system or to otherwise disregard, override or reverse the output"[footnoteRef:51]. This constitutes a statutory "kill switch" with violations attracting fines under Article 99 of up to €15 million or 3% of worldwide annual turnover.

4.4 Case 4: The CoWIN Data Leak via Automated API Scraping (2023)

4.4.1 Factual Matrix

In June 2023, a Telegram bot was found providing, on demand, personal data of CoWIN-registered citizens-including Aadhaar, PAN, and passport numbers-in response to a phone-number query[footnoteRef:52]. MeitY stated CoWIN's data could be accessed via OTP, authorised vaccinators, or third-party APIs, but acknowledged a "trusted API" permitting retrieval without OTP for entities including ICMR[footnoteRef:53]. CERT-In's initial investigation indicated the bot's backend was operating from a "threat actor database… populated with previously stolen data" rather than directly accessing CoWIN APIs[footnoteRef:54], though the Government never conclusively confirmed or denied a direct breach.

4.4.2 Legal Gap: Absence of Data Protection by Design Mandates

The DPDP Act imposes a general obligation to implement "reasonable security safeguards" but does not mandate Data Protection by Design in the GDPR Article 25 sense-architecturally embedded pseudonymisation, anomaly detection, and rate-limiting from the design stage[footnoteRef:55]. The DPDP Act's substantive obligations do not become fully effective until May 2027. CoWIN was built without API rate-limiting, automated anomaly detection, consistent end-to-end encryption, or pseudonymisation of stored personal data.

4.4.3 EU Comparator: GDPR Article 25 and AI Act Continuous Monitoring

GDPR Article 25 mandates, as a binding obligation, appropriate technical measures "both at the time of the determination of the means for processing and at the time of the processing itself." The EU AI Act supplements this for AI-driven platforms by classifying AI systems used in public-service eligibility determinations as potentially "high-risk" under Annex III, Point 5(a), requiring continuous logging and transparency. Under the combined GDPR-AI Act framework, CoWIN would have been required, from the design stage, to incorporate pseudonymisation and automated anomaly-detection algorithms.

4.5 Contextual Data: India's Cybercrime Trajectory (2020-2024)

Table 2 and Figures 2-4 present NCRB and I4C data quantifying the escalation of India's cyber-threat landscape, as published in the Ministry of Home Affairs' PIB release of 21 July 2026[footnoteRef:56].

Table 2. All-India Cyber Crime Cases Registered, 2020-2024

Category	**2020**	**2021**	**2022**	**2023**	**2024**
Total Cyber Crimes	50,035	52,974	65,893	86,420	1,01,928
IT Act Offences	29,643	27,427	31,908	44,237	44,872
IPC/BNS Offences	20,201	25,384	33,798	41,849	56,747
Fraud	10,395	14,007	17,470	19,466	29,758
Cheating	4,480	6,343	10,509	16,943	19,296
Data Theft	98	170	97	113	88
Cyber Terrorism	26	15	12	11	18

Source: NCRB "Crime in India" (2020-2024), as published in PIB Release, 21 July 2026 (PRID: 2287039)

Figure 1. Total Cyber Crime Cases Registered in India, 2020-2024

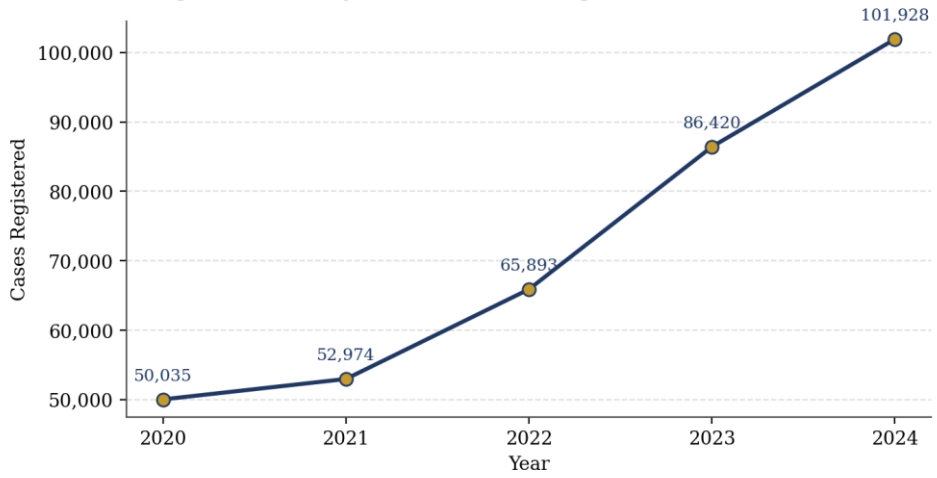

Figure 2. Total Cyber Crime Cases Registered in India, 2020-2024.

Source: Visualisation of NCRB data, PIB Release, 21 July 2026

Overall, this data shows a continued and accelerating growth pattern, with the number of total cases increasing by nearly 200% over five years (CAGR around 19.5%).Figure 3 disaggregates this growth by category, revealing that the increase is not uniform: IPC/BNS offences (which capture fraud, cheating, and related deception) grew fastest in absolute terms, nearly tripling from 20,201 to 56,747 cases.

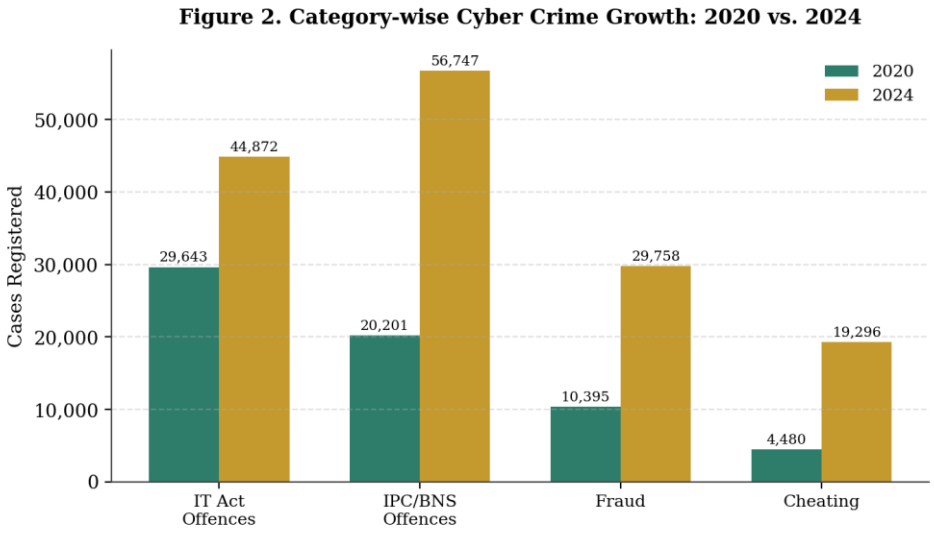

Figure 3. Category-wise Cyber Crime Growth: 2020 vs. 2024.

Source: Author's visualisation of NCRB data, PIB Release, 21 July 2026

The Citizen Financial Cyber Fraud Reporting and Management System (CFCFRMS) operated by I4C has documented over 6.58 million (65.89 lakh) financial-fraud complaints on the NCRP between 2021 and 2025, with total reported losses exceeding INR 55,050 crore, against which more than INR 11,158 crore has been saved as of 30 June 2026[footnoteRef:57]. Figure 4 visualises these three indicators on a common scale.

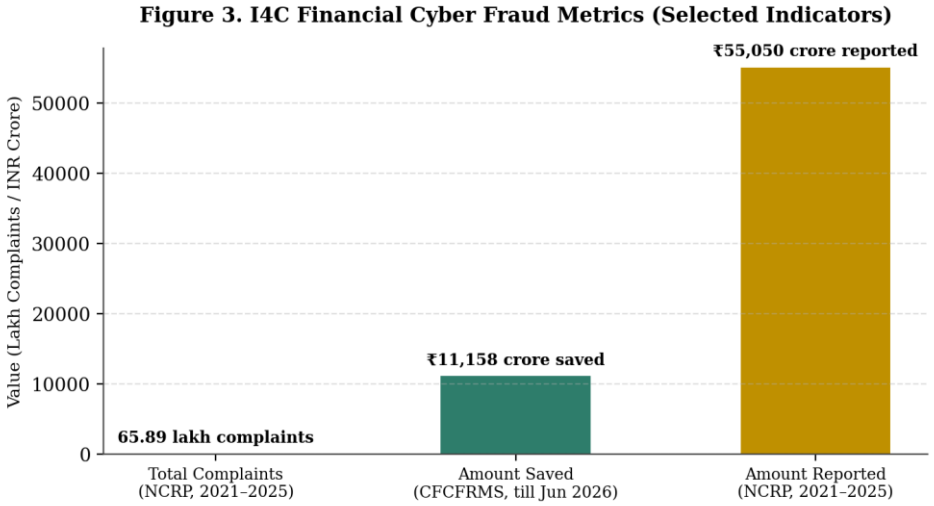

Figure 4. I4C Financial Cyber Fraud Metrics (Selected Indicators).

Source: Author's visualisation of I4C/CFCFRMS data, PIB Release, 21 July 2026

Table 3. Summary: Four-Case Legal Gap Mapping with Reform Priorities

Case	Indian Law Gap	EU Comparator	Sector	Case Type
KKNPP 2019	No supply-chain audit mandate	NIS 2 Art. 21(2)(d)	Nuclear/Energy	AI-Adjacent

AIIMS 2022	No micro-segmentation/pen-testing mandate	NIS 2 Art.21(2)(e-f); AI Act Art.15	Healthcare	AI-Adjacent
Mumbai Grid 2020	No HITL for automated load-dispatch AI	AI Act Art.14; Annex III Pt.2	Energy	AI-Direct
CoWIN 2023	No Data Protection by Design mandate	GDPR Art.25; AI Act Arts.12-13	Digital Public Svc	AI-Adjacent

5. Legislative Reform Blueprint

Drawing upon the comparative legal analysis in Section 3 and the forensic case-study findings in Section 4, this paper proposes a five-pillar legislative reform framework for India. This framework is designed to be implementable either as a standalone Artificial Intelligence (Regulation and Safety) Act or as targeted amendments to the IT Act, 2000 and the DPDP Act, 2023.

5.1 Pillar I: Tiered AI-Risk Classification for CII

To facilitate the implementation of the EU AI Act, a tiered, risk-proportionate classification framework for all AI systems deployed in specific CII sectors should be adopted in India, but with a contextual adaptation. The proposed three-tier classification would include: Tier 1 Critical Risk: AI systems that are components of safety in nuclear, defence, power-grid, air-traffic-control, and other types of important facilities; Tier 2 High Risk: AI systems used as safety components in healthcare diagnostics, financial-system surveillance, biometric-identity-verification and other areas; Tier 3 Moderate Risk: non-safety-critical CII support functions. They would have proportionate compliance requirements, ranging from pre-deployment conformity assessment (Tier 1) to documented risk assessment and summary reporting (Tier 3).

5.2 Pillar II: Mandatory Supply-Chain Cyber-Auditing

India should introduce a statutory supply-chain security obligation, directly modelled on NIS 2 Article 21(2)(d), applicable to all operators of Government-designated CII under Section 70/70A of the IT Act. This should mandate pre-contractual cybersecurity risk assessment of vendors, binding contractual cybersecurity clauses conforming to NCIIPC-prescribed minimum standards, annual third-party supply-chain audits, mandatory subcontractor-register disclosure, and a graduated administrative-penalty framework with personal accountability for management bodies of CII operators.

5.3 Pillar III: Statutory Human-in-the-Loop (HITL) Kill Switch

For all Tier 1 and Tier 2 AI systems deployed within CII, India should mandate a statutory "kill switch" requirement, functionally equivalent to EU AI Act Article 14, requiring designated qualified human operators, real-time human-machine interface monitoring tools, documented escalation protocols, an absolute prohibition on fully autonomous AI-driven operations in Tier 1 sectors, and mandatory post-incident review of all instances of human override.

5.4 Pillar IV: Data Protection by Design for Public-Utility Platforms

The DPDP Act, 2023 should be amended to incorporate a binding "Data Protection by Design and by Default" obligation, functionally equivalent to GDPR Article 25, requiring pseudonymisation integrated from the design stage, automated anomaly-detection on all API endpoints, adaptive API rate-limiting, schema-level data minimisation, mandatory pre-deployment privacy impact assessments, and periodic independent penetration testing for all public-utility digital platforms.

5.5 Pillar V: Institutional Consolidation - A Single Statutory AI-CII Coordinating Authority

The institutional analysis in Section 3.2 shows that Pillars I-IV are difficult to implement in the mosaic model as it exists in India with each agency having a small piece of jurisdiction with no statutory coordination authority. Therefore, this paper suggests the establishment of a fifth pillar, which is also structurally first, by enacting a National AI-Critical Infrastructure Authority (NAICIA).

This proposal builds directly upon-but statutorily strengthens-MeitY's own proposed "AI Governance Group" under the India AI Governance Guidelines[footnoteRef:58], converting it from a non-binding coordination forum into a statutory body with four specific powers that no existing Indian body currently possesses in combination: (a) the power to designate Tier 1/2/3 AI-CII classifications under Pillar I, binding on all sectoral regulators (RBI, IRDAI, TRAI) and on NCIIPC alike; (b) the power to prescribe and enforce minimum supply-chain audit standards under Pillar II, uniformly across sectors, superseding inconsistent sectoral guidance; (c) the power to certify HITL kill-switch compliance under Pillar III for Tier 1 AI-CII deployments, functioning analogously to the EU AI Act's notified-body mechanism; and (d) a statutory duty to resolve jurisdictional conflicts between NCIIPC, CERT-In, and sectoral regulators when an incident spans multiple domains-precisely the coordination failure witnessed in the Mumbai grid incident, where energy-sector regulation (CEA), critical-infrastructure protection (NCIIPC), and cyber incident response (CERT-In) operated without a common accountable authority for the AI-relevant dimensions of the incident.

The NAICIA should be constituted with statutory independence like the Data Protection Board of India under the DPDP Act and members should come from different technical, legal, and sectoral backgrounds with a clear statutory mandate to incorporate or replace the advisory role presently being performed by the proposed (non-statutory) AI Governance Group. Most importantly, this reform does not mean that all existing entities would be eliminated; instead, NCIIPC would still have the responsibility to provide protection under the CII, CERT-In would still be responsible for responding to incidents according to their mandate and sectoral regulators would maintain their power to make rules in each sector, but all these entities would function within the NAICIA's binding authority on AI-risk classification and coordination.

Table 4. Proposed Five-Pillar Legislative Reform Framework for India

Reform Pillar	**Indian Law Amendment**	**EU Model**	**Implementation Mechanism**
I. AI-Risk Classification	New Chapter in IT Act or standalone AI Act	EU AI Act Art. 6 + Annex III	NAICIA as designating authority; 3-tier model
II. Supply-Chain Audit	New S.70C in IT Act	NIS 2 Art. 21(2)(d)	Mandatory annual audits; NAICIA minimum standards; management liability
III. HITL Kill Switch	New S.70D in IT Act or AI Act	EU AI Act Art. 14	Designated human operators; override authority; Tier 1 autonomy prohibition
IV. DPbD Mandate	Amendment to DPDP Act S.8	GDPR Art. 25	Mandatory pseudonymisation; API rate-limiting; anomaly detection
V. Institutional Consolidation	New statutory NAICIA Act or IT Act Chapter	EU AI Office + single Regulation	Statutory NAICIA superseding advisory AI Governance Group; binds NCIIPC/CERT-In/sectoral regulators

5.6 Ancillary: AI Hallucination and Judicial Integrity

The Supreme Court's judgment in Pooja Ramesh Singh v. Jammu and Kashmir Bank Ltd. (2026 INSC 668), delivered on 2 July 2026 by Justices Pamidighantam Sri Narasimha and Alok Aradhe, provides a contemporaneous illustration of AI-specific risks transcending the CII domain[footnoteRef:59]. The Court set aside NCLT and NCLAT judgments after discovering that four of six cited precedents were entirely non-existent and two contained fabricated paragraph content, apparently AI-generated. The Court declared: "A decision of a Court or an adjudicating authority based on material which is fake and hallucinated is no decision at all," adopting a "zero tolerance" standard[footnoteRef:60] and directing the Bar Council of India to constitute a disciplinary committee. This judgment, coupled with the UK's contemporary Pinsent Masons LLP incident61, underscores this paper's core argument: that India's legal landscape is fundamentally ill-equipped to handle the challenges posed by the advent of AI in the realms of cybersecurity and data protection, as well as in judicial proceedings.

5.7 Financial Context: I4C CFCFRMS Performance

As of 30 June 2026, the I4C's CFCFRMS has saved financial value of more than INR 11,158 crore in more than 32.80 lakh complaints. There are seven Joint Cyber Co-ordination Teams situated across the country that target hot spots of cybercrime. More than 1,63,344 police and judicial officers have registered at the CyTrain MOOC Portal. The Cyber Commando programme has identified 281 experts and INR 132.93 crore has been disbursed under the CCPWC scheme for capacity building. These investments are for operational response capacity and don't address sections 3-5 of this paper, which are gaps in the institutional architecture and the legislation.

5.8 Legislative Transplants for India:

What India's CII-AI Framework Should Adopt from EU Legislation

1. Rationale and Structure

This section highlights the specific provisions and institutional arrangements and the principles of regulation in the European Union (EU) harmonised AI-CII governance structure that India will need to adopt, adapt, or transplant into its own legislative framework. The analysis is carried out provision by provision in three EU instruments, namely the NIS 2 Directive (Directive (EU) 2022/2555)62, the EU AI Act (Regulation (EU) 2024/1689)63 and the GDPR (Regulation (EU) 2016/679).)[footnoteRef:61]-Each EU provision was mapped to the relevant Indian legal gap and the Indian legislation that needs to be amended was identified, along with the recommended type of transplant (verbatim, contextually adapted, or structural)

Table 1. Master Mapping: EU Provisions India Should Adopt

Sl. No.	EU Provision	Core Obligation	Indian Gap	Recommended Indian Amendment
1	NIS 2, Art. 21(2)(d)	Mandatory supply-chain security auditing	IT Act S.70/70A: no vendor obligation	Insert new S.70C in IT Act
2	NIS 2, Art. 20(2)	Management body personal liability for cybersecurity	No personal liability for CII management	Amend S.70A Rules or new S.70C proviso
3	NIS 2, Art. 23	Tiered incident reporting (24h/72h/1-month)	CERT-In: flat 6-hour rule for all incidents	Amend CERT-In Directions: tiered by severity
4	EU AI Act, Art. 6 + Annex III	Risk-tiered classification of AI in CII	No AI classification exists	New AI Act or IT Act Chapter IVA
5	EU AI Act, Art. 9	Mandatory risk management system for high-risk AI	No risk-management mandate for AI in CII	Embed in AI Act / IT Act Chapter IVA
6	EU AI Act, Art. 14	Human-in-the-Loop (HITL) oversight with override authority	No HITL mandate for any AI system	New S.70D in IT Act: HITL kill switch
7	EU AI Act, Art. 15	Accuracy, robustness, and cybersecurity for high-risk AI	No technical standards for AI in CII	BIS standards mandated via IT Act / AI Act
8	EU AI Act, Arts. 11-12	Technical documentation and automatic logging	CERT-In 180-day log rule; no AI-specific logging	Extend CERT-In Directions to AI decision logs

9	EU AI Act, Art. 13	Transparency: instructions for use of high-risk AI	No algorithmic transparency mandate	Embed in AI Act / IT Amendment Rules
10	GDPR, Art. 25	Data Protection by Design and by Default	DPDP Act S.8(5): only "reasonable security"	Amend DPDP Act S.8: insert DPbD mandate
11	GDPR, Art. 35	Data Protection Impact Assessment (DPIA)	No mandatory DPIA for public-utility platforms	Amend DPDP Act: mandatory DPIA for SDFs
12	EU AI Act, Art. 64 + EU AI Office	Central coordination authority for AI governance	11-body mosaic; no central AI authority	Statutory NAICIA (proposed)

Source: Compiled by author from NIS 2, EU AI Act, GDPR, IT Act 2000, DPDP Act 2023, and CERT-In Directions 2022.

2. Detailed Adoption Recommendations

2.1 Supply-Chain Security Auditing (from NIS 2, Article 21(2)(d))

What the EU provision requires

NIS 2 Article 21(2)(d) mandates that essential and important entities implement cybersecurity risk-management measures addressing "security-related aspects concerning the relationships between each entity and its direct suppliers or service providers." Commission Implementing Regulation (EU) 2024/2690 specifies that this includes: formalised supplier risk-assessment methodologies; contractual security clauses reflecting the entity's risk profile; continuous monitoring of supplier cybersecurity posture; and mandatory incident-notification cascading[footnoteRef:62]. Non-compliance attracts fines of up to €10 million or 2% of worldwide annual turnover (Art. 34(4)). Article 20(2) imposes personal liability on management bodies for failure to oversee implementation.

What India currently lacks

Section 70 of the IT Act designates "Protected Systems" but imposes no obligation on the vendors, contractors, and service providers who access, service, or maintain those systems. NCIIPC's Guidelines address vendor management advisorily, but carry no statutory force and prescribe no penalties. The Kudankulam nuclear plant malware entered through a third-party contractor's PC connected to the administrative network - a scenario that would have been forestalled had binding vendor-auditing obligations existed.

Recommended Indian transplant

Insert a new Section 70C in the IT Act ("Supply-Chain Security Obligations for Protected Systems"), mandating that every operator of a designated Protected System under Section 70 shall: (a) conduct documented pre-contractual cybersecurity risk assessments of all vendors accessing any component of the Protected System's network; (b) include binding contractual cybersecurity clauses conforming to minimum standards prescribed by NCIIPC; (c) perform annual third-party supply-chain audits by NCIIPC-empanelled auditors, with results reported to the sectoral regulator within 30 days; (d) maintain a vendor dependency register, updated quarterly, disclosing each Tier-1 supplier's own critical technology dependencies; and (e) report any supply-chain-originating cyber incident to CERT-In within 6 hours and to the sectoral regulator within 24 hours. Non-compliance should attract penalties mirroring Section 70(3)'s existing imprisonment/fine framework, with an additional administrative penalty of up to INR 25 crore for systemic vendor-management failures[footnoteRef:63]. A proviso to Section 70C should establish personal liability for the designated CISO or equivalent officer of the CII operator for wilful or grossly negligent failure to implement supply-chain audit procedures-mirroring NIS 2 Article 20(2)'s management-accountability principle.

2.2 Human-in-the-Loop Kill Switch (from EU AI Act, Article 14)

What the EU provision requires

Article 14 of the EU AI Act mandates that high-risk AI systems (including those deployed in critical infrastructure under Annex III, Point 2) be "designed and developed in such a way, including with appropriate human-

machine interface tools, that they can be effectively overseen by natural persons during the period in which they are in use" (Art. 14(1)). Article 14(3) requires that human oversight include, at minimum, the ability to: fully understand the system's capacities and limitations; remain aware of automation bias; and correctly interpret the system's output. Article 14(4) requires that the designated person have authority to "decide, in any particular situation, not to use the high-risk AI system or to otherwise disregard, override or reverse the output"[footnoteRef:64].

What India currently lacks

No Indian statute, regulation, or guideline requires human oversight of any AI-driven decision in any critical-infrastructure sector. The CEA Cyber Security in Power Sector Guidelines, 2021 address conventional IT controls (firewalls, intrusion detection, access management) but do not address the specific risk of algorithmic manipulation of automated load-dispatch or grid-management systems. The 2020 Mumbai power grid incident demonstrated that adversaries (RedEcho/ShadowPad) accessed SCADA-adjacent systems controlling load dispatch - systems that increasingly integrate AI-driven predictive algorithms. Indian law neither requires nor provides a mechanism for human operators to override or halt such algorithmic decisions.

Recommended Indian transplant

Insert a new Section 70D in the IT Act ("Mandatory Human Oversight of Automated Decision Systems in Protected Systems"), or equivalently, a chapter in a proposed standalone AI (Regulation and Safety) Act. This provision should mandate: (a) designation of a qualified human operator, with demonstrated competence certified by the relevant sectoral regulator, for every AI or automated decision system deployed within a Protected System; (b) real-time monitoring interfaces enabling the operator to observe the AI system's outputs, confidence levels, and anomaly indicators; (c) documented authority and technical capability for the operator to override, halt, or reverse any AI-generated output in any scenario; (d) mandatory escalation protocols specifying conditions under which override is compulsory (e.g., variance in load-dispatch signals exceeding a prescribed threshold, diagnostic confidence below a prescribed floor, detection of anomalous data-input patterns); (e) an absolute prohibition on fully autonomous AI operations in Tier 1 (Critical Risk) sectors - no AI system may execute a safety-critical action (reactor-control adjustment, grid switching, load shedding) without either prior human approval or a concurrent human-monitoring failsafe; and (f) mandatory post-incident documentation and review of every instance of human override, reported to NCIIPC and the sectoral regulator within 72 hours.

2.3 Tiered AI-Risk Classification for CII (from EU AI Act, Article 6 + Annex III)

What the EU provision requires

The EU AI Act establishes a four-tier risk classification: unacceptable risk (prohibited, Art. 5), high risk (Arts. 6-27), limited risk (Art. 50), and minimal risk. Article 6, read with Annex III, classifies AI systems used as safety components of, or embedded within, critical infrastructure - including digital infrastructure, road traffic, water, gas, heating, and electricity - as "high-risk" systems subject to the most stringent compliance obligations: risk management (Art. 9), data governance (Art. 10), technical documentation (Art. 11), logging (Art. 12), transparency (Art. 13), human oversight (Art. 14), and accuracy/robustness/cybersecurity (Art. 15)[footnoteRef:65].

What India currently lacks

India has no AI-specific legislation whatsoever - enacted, notified, or in advanced draft. The IT Act, 2000 does not mention "artificial intelligence," "machine learning," "automated decision-making," or "algorithm." The DPDP Act, 2023, addresses data protection but not AI-system safety. The IT Amendment Rules 2026 address AI-generated synthetic content (deepfakes) for content-moderation purposes but do not regulate AI systems as safety-critical components within CII. The IndiaAI Mission funds AI innovation but exercises no regulatory or enforcement function. The private member's Artificial Intelligence (Ethics and Accountability) Bill, 2025 has not been enacted and lacks Government sponsorship. The proposed Digital India Act remains in consultation with no enacted text. There is, in short, no classification of AI systems by risk level, no enumeration of sectors in which AI deployment triggers enhanced obligations, and no pre-deployment conformity assessment for any AI system deployed in any CII sector.

Recommended Indian transplant

Enact a standalone Artificial Intelligence (Regulation and Safety) Act, or insert a new Chapter IVA ("Regulation of Artificial Intelligence Systems in Critical Information Infrastructure") into the IT Act. This chapter should establish a three-tier risk classification contextually adapted from the EU's four-tier model (merging the EU's "unacceptable" and "minimal" tiers, which are less relevant in the CII-specific context):

Table 2. Proposed Three-Tier AI-Risk Classification for Indian CII

Tier	Sectors / Applications	Compliance Obligation	EU Equivalent
Tier 1 - Critical Risk	AI in nuclear reactor control, defence systems, power-grid load dispatch (SLDC/RLDC), air traffic control, dam/water SCADA	Pre-deployment conformity assessment by NAICIA/designated notified body; HITL kill switch (S.70D); annual re-assessment; no full autonomy	EU AI Act, Annex III Point 2 + Arts. 9-15 (full compliance)
Tier 2 - High Risk	AI in healthcare diagnostics/triage, financial-system surveillance, biometric identity platforms (Aadhaar-linked), public-utility digital platforms (CoWIN-type)	Self-assessed compliance with BIS-prescribed standards, auditable by sectoral regulator; HITL oversight recommended; DPbD mandatory	EU AI Act, Annex III Points 1, 5 + Arts. 9-15 (proportionate)
Tier 3 - Moderate Risk	AI in predictive maintenance, administrative scheduling, non-biometric analytics, energy-demand forecasting (advisory, not operational)	Documented risk assessment; summary reporting to NCIIPC; transparency notice to affected users	EU AI Act, Art. 50 (limited risk / transparency)

2.4 Data Protection by Design and by Default (from GDPR, Article 25)

What the EU provision requires

GDPR Article 25(1) mandates that data controllers "shall, both at the time of the determination of the means for processing and at the time of the processing itself, implement appropriate technical and organisational measures, such as pseudonymisation, which are designed to implement data-protection principles, such as data minimisation, in an effective manner and to integrate the necessary safeguards into the processing." Article 25(2) extends this to "data protection by default": the controller must ensure that, by default, only personal data necessary for each specific purpose is processed. This is not advisory - violations attract fines under Art. 83(5) of up to €20 million or 4% of worldwide annual turnover[footnoteRef:66].

What India currently lacks

The DPDP Act, 2023, Section 8(5), imposes only a general obligation to implement "reasonable security safeguards to prevent personal data breach." The DPDP Rules, 2025 elaborate this as encryption, access controls, data backups, and retention for at least one year - but these are enumerated as examples of reasonable measures, not as architectural mandates that must be embedded at the design stage. There is no obligation to pseudonymise data at rest, no obligation to implement automated anomaly detection on API endpoints, no obligation to conduct privacy impact assessments before deployment, and no obligation to minimise data collection at the schema level. The CoWIN incident showed the reality – there was no rate limiting or anomaly detection, no pseudonymisation of hundreds of millions of citizens' biometric and identity data was built to serve as a public-utility platform.

Recommended Indian transplant

Amend Section 8 of the DPDP Act, 2023 by inserting a new sub-section 8(5A) ("Data Protection by Design and by Default"), providing that every data fiduciary, and every Significant Data Fiduciary in particular, shall implement appropriate technical and organisational measures at the time of determining the means for processing and throughout the processing itself, including but not limited to: (a) pseudonymisation or tokenisation of personal data at rest and in transit, integrated from the software-architecture design stage; (b) automated anomaly-detection systems on all API endpoints, capable of identifying and blocking mass-query, scraping, enumeration, and brute-force access patterns in real time; (c) adaptive API rate-limiting with configurable, context-sensitive thresholds; (d) data minimisation enforced at the database-schema level, limiting collection and retention to the operational minimum; (e) mandatory data protection impact assessments (DPIAs, borrowing from GDPR Art. 35) for all public-utility digital

platforms before deployment, documented and auditable by the Data Protection Board; and (f) periodic independent penetration testing and red-teaming at intervals prescribed by the Data Protection Board, with results reported to CERT-In. Non-compliance with sub-section 8(5A) should attract the same penalty regime as sub-section 8(5) - up to INR 250 crore under the existing DPDP penalty schedule.

2.5 Management Body Personal Liability (from NIS 2, Article 20(2))

What the EU provision requires

NIS 2 Article 20(1) requires that "the management bodies of essential and important entities approve the cybersecurity risk-management measures taken by those entities in order to comply with Article 21 and oversee its implementation." Article 20(2) specifies that "members of the management bodies of essential and important entities are required to follow training" and "shall encourage essential and important entities to offer similar training to their employees on a regular basis." Crucially, management bodies can be held personally liable for infringements of Article 21[footnoteRef:67].

What India currently lacks

The IT Act's Section 85 provides for vicarious liability of "every person who, at the time the contravention was committed, was in charge of, and was responsible to, the company for the conduct of business" - but this is a general corporate-liability provision, not specific to cybersecurity governance of CII. There is no requirement that CII management bodies personally approve cybersecurity risk-management measures, undergo mandatory cybersecurity training, or bear personal accountability for systemic failures in AI-CII governance. In the KKNPP incident, there is no public record of any management-level officer of NPCIL or NCIIPC being held personally accountable for the supply-chain vulnerability that enabled the intrusion.

Recommended Indian transplant

Insert a proviso to the proposed Section 70C (or include within the proposed AI Act) establishing that the Board of Directors or equivalent governing body of every CII operator shall: (a) formally approve the cybersecurity and AI-risk management measures adopted under Sections 70C and 70D; (b) oversee implementation through a designated sub-committee with a minimum of one member possessing demonstrated cybersecurity expertise; (c) undergo mandatory annual cybersecurity and AI-governance training, certified by NCIIPC or a NCIIPC-empanelled institution; and (d) bear personal liability for wilful or grossly negligent failure to approve, oversee, or implement the required measures, with penalties including disqualification from holding office in any CII-operating entity for a period of up to five years.

6. Conclusions

This paper aimed to assess the current laws, regulations, and policy gaps in India's Critical Information Infrastructure (CII) protection framework concerning the deployment of Artificial Intelligence (AI), and to propose a comprehensive, risk-based legislative framework based on the collective principles and frameworks of the EU's harmonised regulatory system. Through a doctrinal and comparative legal methodology applied across four forensic case studies-the 2019 Kudankulam Nuclear Power Plant Dtrack malware intrusion[footnoteRef:68], The recent AIIMS New Delhi ransomware attack and the Mumbai power grid outage in 2020 are two such examples. The 2022 AIIMS New Delhi ransomware attack and the 2020 power grid outage in Mumbai are just two such occurrences.

The comparative analysis indicates that there are five major voids in India's policy landscape of AI, critical infrastructure and their regulation, and all of these gaps have a more developed counterpart in the regulatory system of the European Union. Second, the Information Technology Act, 2000 (the "Act") does not place a statutory requirement for operators of a designated Protected System to conduct audits of supply chains for cybersecurity. The leakage of the Dtrack malware into the Kudankulam Nuclear Power Plant (KKNPP) was due to the regulator's oversight and allowed the malware to be introduced via an internet-connected computer belonging to a third-party contractor of the plant. Article 21(2)(d) of the NIS 2 Directive – and the corresponding implementing regulation – rather explicitly requires supply-chain security risk management. Second, the country does not have any mandate to perform network micro-segmentation, ex-ante penetration testing and Cyber Security robustness in Healthcare institutions categorised under the Critical Information Infrastructure (CII). As witnessed in the case of AIIMS ransomware attack, a thirty-year-old, outmoded, and not segmented IT environment was used as breeding ground for LockBit malware spreading. In contrast, Article 21(2)(e) and 21(2)(f) of the NIS 2 Directive mandate systematic management of vulnerabilities and periodic evaluation of the effectiveness of cybersecurity and Article 15 of the EU

AI Act requires eligibility criteria for high-risk AI systems, including robustness and resilience and cybersecurity requirements. Thirdly, the legislative framework in India doesn't have any mandates for human-in-the-loop (HITL) oversight over AI-powered decision-making or algorithmic decision-making in critical infrastructure industries. As a result, AI systems, such as power-grid load-dispatch applications, might not require legally mandated human override or emergency shutdown feature. This shortcoming is addressed in the EU AI Act in Article 14, where provisions stipulate that high-risk AI systems used in critical infrastructure must include effective human oversight and human override mechanisms. Finally, the Digital Personal Data Protection Act, 2023 lacks the concept of binding Data Protection by Design and Data Protection by Default. Section 8(5), on the contrary, leaves data fiduciaries with the ability to use "reasonable security safeguards. The shortcomings of such an approach were seen with the CoWIN platform, which did not provide some of the fundamental privacy preserving and security by design features such as API rate limiting, automated anomaly detection and pseudonymisation. By contrast, GDPR 25(1) includes a specific and reminiscently prescriptive requirement such that data protection principles are “by design and by default”, integrated with information systems. Lastly, there is no central agency in India with the statutory mandate to implement these regulatory requirements uniformly among the multitude of regulatory agencies (as highlighted in Section 3.2 and Figure 1), within the framework of AI governance. The institutional fragmentation is a stark contrast to the European Union's very centralized system of governance, where the AI Act is a directly binding regulation that applies to all Member States and the EU AI Office provides a forum for a coordinated application and enforcement of the AI Act by national authorities.

As illustrated in Section 5.8, these five structural failures are not analytical categories, but can be translated, provision by provision, into twelve distinct legislative transplants from the NIS 2 Directive, the EU AI Act and the GDPR. The Legislative Transplants analysis (Section 5.8) outlines how every EU provision relates to the applicable Indian legislation that needs to be amended, including new Section 70C to the IT Act for compulsory supply chain auditing, new Section 70D to the IT Act for a statutory HITL kill switch, amended Section 8 of the DPDP Act to include Data Protection by Design, and the introduction of a National AI-Critical Infrastructure Authority (NAICIA) to replace the current non-binding, eleven-body coordination vacuum. It is crucial to note that this paper does not endorse the blanket importation of EU law to India. The three-tier AI-risk classification presented in Table 2 (Section 5.8) is adapted in context from the EU’s four tiers and combines tiers 2 and 3, ‘unacceptable' and ‘minimal' respectively, which are less operationally relevant for India's threat context and aligns tier 1 with sectors that are more relevant to India's threat context than the EU's Annex III. Likewise, the proposed NAICIA takes structural cues from the EU-Building the AI Office but is intended to function within the existing institutional structure in India. NCIIPC will continue to have the mandate of Section 70A, while CERT-In shall continue to have the mandate of Section 70B and domain-specific rule makers will continue to have the rule-making power over the aspects related to AI. NAICIA will retain the mandates of binding coordination powers over aspects related to AI which are not currently covered by any specific body.[footnoteRef:69].

Another contribution of this paper is methodological. The Scope Note for Section 2.1 carefully examines the distinction between AI-direct and AI-adjacent case evidence, as has been done in the “Case Type” column of Table 3. The Mumbai power grid case is discussed as AI-direct: Here the legal gap (HITL) is how the algorithmic control of load-dispatch decisions is considered, i.e. actual or prospective. The KKNPP, AIIMS and CoWIN cases are analysed as AI-adjacent: they were each in their historical context a simple malware, ransomware or data-scraping event, each revealing structural conditions which are either vendor accountability or architectural resilience, and design-stage privacy, without which any future deployment of AI in those sectors would be exposed to the same vulnerabilities. Because this methodological transparency enhances and doesn't detract from the inferential claims of the paper, it is a good thing.

There are two streams of evidence that converge in their urgency to make the proposed reforms. The quantitative data presented in Section 4.5 and Figures 2-4, extracted from NCRB sources reports titled “Crime in India” (2020-2024) as released in PIB on 21 July 2026, indicates the total number of cyber crimes reported has doubled from 50,035 in 2020 to 101,928 in 2024 (CAGR ~19.5%) and cyber-fraud cases have tripled from 10,395 in 2020 to 29,758 in 2024, with cumulative financial-fraud losses reported at the National Cyber Crime Reporting Portal (NCCRP) between 2021 and 2025 in excess of INR 55,050 crore. This data shows that the I4C's CFCFRMS has successfully saved more than INR 11,158 crore in complaints valued at over INR 32.80 lakh; has trained more than 281 Cyber Commandos and commissioned forensic laboratories in 33 States/UTs; which indicates that India's operational response capability is growing, but at the same time, it also implies that the legislative framework in which these operational investments operate is structurally lagging behind the threat trajectory it seeks to counter.

The qualitative aspect of this urgency can be seen in the Supreme Court judgement in Pooja Ramesh Singh v. Jammu and Kashmir Bank Ltd. (2026 INSC 668).[footnoteRef:70], which is set aside NCLT and NCLAT judgments after they found that the adjudicating order relied on AI-generated hallucinated content, which included four non-existent judgments and two fabricated paragraphs as judicial precedents. While the 'zero tolerance' statement by the Court and the instruction to the Bar Council of India to draft norms for discipline make clear that the threat of AI has seeped into Indian adjudicatory processes, it's not just critical infrastructure sectors. This is not a potential danger; it's an actual danger, evidenced in a court of law.

The structural failure in India's "multi-agency mosaic model" where the powers related to AI-governance are spread across a number of agencies without a binding mechanism of coordination, is prior to and before the four substantive gaps identified above. If the supply-chain audit mandate (Pillar II) is to be applied uniformly, then it will be difficult to make it work if the various regulators that may have jurisdiction over vendors have different or even nonexistent requirements. The only way to have a kill switch in practice for HITL is to have an incident across the energy, cybersecurity, and national security domains across the CEA, NCIIPC, CERT-In and no clearly designated authority of the government on AI. No Data Protection by Design mandate (Pillar IV) is going to be architecturally effective if each agency – Data Protection Board, CERT-In and sectoral regulator – has partial, overlapping, and uncoordinated jurisdiction in the same public-utility digital platform. For this reason, Pillar V – the statutory constitution of NAICIA – is not considered a fifth reform, but rather the structurally prior precondition for the coherence and enforceability of Pillars I – IV. There are some limitations to this paper. While the four case studies are sectorally representative, classified government investigation reports (where available) were not accessible. The EU's regulatory model is not the easiest to implement, as only 23 out of 27 Member States have been subject to infringement proceedings for the lack of transposition of NIS 2 by the deadline in October 2024, highlighting the fact that enacted legislation does not necessarily mean effective implementation of the regulations. Comparative analysis of the proposed three-tier conformity-assessment system with other non-EU jurisdictions (such as the United States' NIST AI Risk Management Framework, Singapore's Model AI Governance Framework, and China's Interim Measures for the Management of Generative AI Services) should be conducted to enrich the transplant analysis beyond the EU-India dyad, and the fiscal and human-capital requirements for implementing the proposed three-tier conformity-assessment system across India's CII landscape should be explored in detail alongside the institutional design of NAICIA and the potential for its relationship with the proposed Digital India Act, and the pending AI Ethics and Accountability Bill, 2025.

Overall, this paper has shown that the Information Technology Act, 2000, the Digital Personal Data Protection Act, 2023, the CERT-In Directions of 2022, the CEA Cyber Security Guidelines, and the NCIIPC Guidelines do not, individually and collectively, have the structural capacity to control the deployment and use of AI within the critical infrastructure of India with risk-proportionate, supply-chain-aware, human-overseen, privacy-by-design, and institutionally coordinated governance. Drawing on experience from the EU's NIS 2 Directive, the AI Act and the GDPR, twelve specific legislative transplants have been identified and contextually adapted for Indian adoption, which is a tried and tested regulatory model that is architecturally coherent and operationally tested. The five pillar reform framework is a coherent and progressive legislative package that could be put into practice and is tiered according to AI-risk classification, the mandatory supply-chain auditing with management accountability, statutory HITL kill switches, Data Protection by Design mandates, and institutional consolidation of a National AI-CII Authority. This vision of India being a global leader in digital technology, manifest in the Digital India programme, IndiaAI Mission and INR 10,371.92 crore investment in AI compute and safety infrastructure does not fit within the regulatory environment of the pre-AI era and the eleven uncoordinated regulators. The research goal of this paper has been achieved: the legal, regulatory and systemic gaps have been assessed and a coherent legislatively structured plan for management of risk has been proposed based on the governance lessons from the EU and taken into account the institutional realities in India. All that's left now is the political will to make it.

List of Abbreviations

AI	Artificial Intelligence
AIIMS	All India Institute of Medical Sciences
BIS	Bureau of Indian Standards
CERT-In	Indian Computer Emergency Response Team

CFCFRMS	Citizen Financial Cyber Fraud Reporting and Management System
CII	Critical Information Infrastructure
DPbD	Data Protection by Design
DPDP Act	Digital Personal Data Protection Act, 2023
GDPR	General Data Protection Regulation
HITL	Human-in-the-Loop
I4C	Indian Cyber Crime Coordination Centre
ICS	Industrial Control Systems
IRDAI	Insurance Regulatory and Development Authority of India
KKNPP	Kudankulam Nuclear Power Plant
MeitY	Ministry of Electronics and Information Technology
NAICIA	National AI-Critical Infrastructure Authority (proposed)
NCIIPC	National Critical Information Infrastructure Protection Centre
NCRP	National Cyber Crime Reporting Portal
NIS 2	Network and Information Security Directive 2 (EU)
NPCIL	Nuclear Power Corporation of India Limited
RBI	Reserve Bank of India
SCADA	Supervisory Control and Data Acquisition
SLDC/RLDC	State/Regional Load Despatch Centre
TRAI	Telecom Regulatory Authority of India

References

1. A. Van Dine, M. Assante, P. Stoutland. “Outpacing Cyber Threats: Priorities for Cybersecurity at Nuclear Facilities,” Nuclear Threat Initiative, 2016. https://media.nti.org/documents/NTI_CyberThreats__FINAL.pdf
2. Supreme Court of India. Pooja Ramesh Singh v. Jammu and Kashmir Bank Ltd. & Anr., Civil Appeal No. 11950 of 2025 (2026 INSC 668), decided 02 July 2026.
3. Maj Gen P.K. Mallick, VSM (Retd). “Cyber Attack on Kudankulam Nuclear Power Plant - A Wake Up Call.” VIF Paper, Vivekananda International Foundation, New Delhi, December 2019. ISBN: 978-81-943795-2-2.
4. TAC Security. “Ransomware Attack at AIIMS: NIA Suspects Cyberterrorism.” November 30, 2022. https://tacsecurity.com/ransomware-attack-at-aiims-nia-suspects-cyberterrorism/
5. Recorded Future, Insikt Group. “China-Linked Group RedEcho Targets the Indian Power Sector Amid Heightened Border Tensions.” February 2021. https://www.recordedfuture.com/research/continued-targeting-of-indian-power-grid-assets
6. The South First. “Report Says CoWIN Security Breach Bleeds Personal Data.” June 12, 2023. Available at: https://thesouthfirst.com/health/cowin-security-breach-leaks-personal-data-says-report-opposition-parties-raise-safety-questions/
7. Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 (NIS 2 Directive). OJ L 333, 27.12.2022, pp. 80-152. https://eur-lex.europa.eu/eli/dir/2022/2555
8. Regulation (EU) 2024/1689 of the European Parliament and of the Council (EU AI Act). OJ L, 12.07.2024. https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=OJ:L_202401689
9. Regulation (EU) 2016/679 (GDPR). OJ L 119, 04.05.2016. Available at: https://eur-lex.europa.eu/eli/reg/2016/679
10. Ministry of Home Affairs, Government of India. “National Cyber Crime Data.” PIB, 21 July 2026, PRID 2287039. Available at: https://www.pib.gov.in/PressReleasePage.aspx?PRID=2287039

11. The Information Technology Act, 2000 (India), Sections 43, 43A, 66F, 70, 70A, 70B. https://www.indiacode.nic.in/
12. NCIIPC. Guidelines for the Protection of National Critical Information Infrastructure. https://www.nciipc.gov.in/
13. CERT-In. Directions under Sub-section (6) of Section 70B of the Information Technology Act, 2000. 28 April 2022.
14. SentinelOne. "What Is NIS2? EU Cybersecurity Directive Explained." May 2026. https://www.sentinelone.com/cybersecurity-101/cybersecurity/what-is-nis2/
15. Springlex. "Art. 21 Cybersecurity Risk-Management Measures, NIS 2 Directive." https://www.springlex.eu/en/packages/nis2/nis2-directive/article-21/
16. Commission Implementing Regulation (EU) 2024/2690 of 17 October 2024. https://www.nis-2-directive.com/NIS_2_Directive_Article_21.html
17. EY. "How Will NIS2 Affect the Supply Chain Security Approach?" September 2025. https://www.ey.com/en_pl/insights/law/nis2-supply-chain-security
18. artificialintelligenceact.eu. "High-Level Summary of the AI Act." https://artificialintelligenceact.eu/high-level-summary/
19. Kaspersky Labs. "DTrack: Previously Unknown Spy-Tool by Lazarus." September 23, 2019. https://usa.kaspersky.com/about/press-releases/2019_dtrack-previously-unknown-spy-tool-hits-financial-institutions-and-research-centers
20. S. Datta, A. Salmon. "North Koreans Behind Indian Nuclear Plant Hack." Asia Times, November 12, 2019. https://www.asiatimes.com/2019/11/article/north-koreans-behind-indian-nuclear-plant-hack/
21. Sensecy (Verint). "Cyber Threat Intelligence Alert: Indian Nuclear Power Plant Attacked with Dtrack Malware." November 2019.
22. ACE Cloud Hosting. "AIIMS Cyberattack 2022: Shielding India's Healthcare." April 2025. https://www.acecloudhosting.com/blog/aiims-cyberattack-2022/
23. CM Alliance. "AIIMS Ransomware Attack Timeline."https://www.cm-alliance.com/cybersecurity-blog/aiims-ransomware-attack
24. Lukmaan IAS. "Cyberattack on CI Infrastructure: AIIMS Case Study." March 2023. https://blog.lukmaanias.com/2023/03/22/topic-cyberattack-on-critical-information-ci-infrastructure-a-case-study-of-ransomware-on-aiims/
25. Business Today. "Cyber Attack from China Behind Mumbai Power Outage." March 1, 2021. https://www.businesstoday.in/latest/economy-politics/story/cyber-attack-from-china-behind-mumbai-power-outage-in-2020-289648-2021-03-01
26. Tribune India. "Cyber Attack, Sabotage Behind 2020 Mumbai Power Outage: Raut." https://www.tribuneindia.com/news/nation/cyber-attack-sabotage-behind-2020-mumbai-power-outage-raut-219084
27. Deccan Herald. "Mumbai Power Outage Due to Human Error: Union Power Minister." March 2, 2021.
28. Idaho National Laboratory, CyOTE Programme. "Precursor Analysis Report: Mumbai 2020 Power Outage." INL/RPT-22-69764. https://cyote.inl.gov/
29. Central Electricity Authority. Cyber Security in Power Sector Guidelines, 2021.
30. The Digital Personal Data Protection Act, 2023 (India), Section 8(5).
31. DLA Piper. "Data Protection Laws - India." https://www.dlapiperdataprotection.com/?t=law&c=IN
32. NITI Aayog. "National Strategy for Artificial Intelligence: #AIforAll." June 2018. https://www.niti.gov.in/
33. NITI Aayog. "Responsible AI for All: Approach Document for India," Parts I-II. February and August 2021.
34. IMPRI Impact and Policy Research Institute. "IndiaAI Mission (2024): Empowering Innovation, Infrastructure, and Inclusive Growth Through AI." March 6, 2025. https://www.impriindia.com/insights/indiaai-mission-2024/
35. Vision IAS. "India AI Governance Guidelines." Current Affairs, March 2026. https://visionias.in/current-affairs/monthly-magazine/2025-12-23/polity-and-governance/india-ai-governance-guidelines
36. Chambers and Partners. "Government Notifies Information Technology Amendment Rules 2026." February 2026. https://chambers.com/articles/government-notifies-information-technology-amendment-rules-2026
37. P. Mali. "AI Laws and Regulations in India as of 2026: A Comprehensive Overview." https://www.prashantmali.com/cyber-law-blog-india/ai-laws-and-regulations-in-india-as-of-2026
38. Business Software Alliance. "India: Five Ways to Bolster the Digital India Act." https://www.bsa.org/policy-filings/india-five-ways-to-bolster-the-digital-india-act
39. Sanskriti IAS. "The Proposed 'Digital India Bill' for a Future-Ready Digital India." https://www.sanskritiias.com/current-affairs/the-proposed-digital-india-bill-for-a-future-ready-digital-india
40. UNESCO Global AI Ethics and Governance Observatory. "India." February 2026. https://www.unesco.org/ethics-ai/en/india
41. Anthony Malcolm Cork & Anor v. Mark Smith, [2026] EWHC 1199 (Ch).
42. Law Society Gazette. "Pinsents' Botched AI Use Sparks Dependency Alarm." 2026. https://www.lawsociety.ie/gazette/top-stories/2026/may/pinsents-botched-ai-use-sparks-dependency-alarm/