REGULATING AI-ASSISTED CYBER THREATS IN INDIA: ASSESSING THE ADEQUACY OF CERT-IN'S EMERGING CYBERSECURITY FRAMEWORK

Shaurya Raj, LL.M., National Law University Jodhpur

ABSTRACT

This project examines whether the Indian Computer Emergency Response Team's ("CERT-In") emerging framework for AI-assisted cyber threats built primarily through advisories and a nonbinding Blueprint issued on 25 May 2026, rather than through binding directions or statutory amendment is an adequate regulatory response to the threat it describes. Drawing directly on CERT-In's AI-specific advisories, the Information Technology Act, 2000, the Digital Personal Data Protection Act, 2023, recent orders of the Supreme Court and the Delhi and Bombay High Courts on deepfake and "digital arrest" fraud, and comparable instruments from the European Union, the United Kingdom and the United States, this project finds that CERT-In's technical diagnosis is current and, in key respects, more demanding than comparable foreign instruments, but that it lacks the binding legal architecture, proportionate penalty structure, and accompanying criminal-law reform needed to convert that diagnosis into enforceable regulation. It concludes with calibrated recommendations for closing this gap.

1. RESEARCH PROBLEM

CERT-In has responded to AI-assisted cyber threats almost entirely through advisories and a Blueprint issued under its general advisory function, rather than through binding directions carrying the statutory penalty structure of Section 70B(6)-(7) of the Information Technology Act, 2000 ("IT Act"), or through legislative amendment. The Blueprint itself concedes that it is "not a binding document" and that its recommendations are to be implemented "in a risk-informed manner." This produces a structural tension between the technical maturity of CERT-In's threat assessment which describes risks of "cascading compromise" and harm to "broader national security" and the comparatively modest legal form of the instrument through which that assessment is communicated. This project examines that tension.

2. RESEARCH OBJECTIVES

1. To examine the statutory basis and legal character of CERT-In's AI-specific instruments.

2. To analyse judicial responses to AI-assisted cyber harm in the continued absence of AI-specific legislation.

3. To compare CERT-In's Blueprint with binding and quasi-binding cybersecurity approaches taken in the European Union, the United Kingdom and the United States.

4. To assess whether CERT-In's framework, taken as a whole, is an adequate regulatory response to AI-assisted cyber threats.

5. To recommend calibrated reforms capable of closing the gaps identified.

3. RESEARCH METHODOLOGY

This project adopts a doctrinal and comparative methodology, built directly on primary texts: the Information Technology Act, 2000; the CERT-In Directions of 28 April 2022; CERT-In Advisories CIAD-2023-0015, CIAD-2025-0013 and CIAD-2026-0020; the Blueprint of 25 May 2026; the Digital Personal Data Protection Act, 2023 and Rules, 2025; reported and unreported orders of the Supreme Court and the Delhi and Bombay High Courts; and the primary texts of the EU AI Act, the UK AI Cyber Security Code of Practice, and NIST/CISA guidance.

4. REVIEW OF LITERATURE

Indian doctrinal literature on cybersecurity law has concentrated on the 2022 CERT-In Directions and the DPDP Act's compatibility with the GDPR and does not yet address CERT-In's 2025-26 AI-specific instruments, which postdate most published commentary. Scholarship following the Srikrishna Committee Report addresses the constitutional foundations of Indian data law but predates frontier AI's emergence as an independent cyber-threat vector. International literature on frontier-model cyber risk, including published assessments by the UK AI Security Institute, is technically rich but does not engage with Indian law, while Indian commentary on the digitalarrest litigation remains confined largely to legal-news coverage rather than peer-reviewed analysis. This project reads CERT-In's newest instruments against both the Indian constitutional backdrop and the comparative frontier-AI-governance literature.

5. INTRODUCTION

Artificial intelligence has, within roughly three years, moved from a speculative concern to a documented feature of India's cyber-threat landscape. The Indian Computer Emergency Response Team ("CERT-In"), the nodal agency constituted under Section 70B of the IT Act, has issued three successive instruments addressing AI-related cyber risk since March 2025, culminating in the Blueprint.[1]

This escalating regulatory attention has not been abstract. CERT-In's own advisory of April 2026 recorded that frontier AI systems can now autonomously discover vulnerabilities across large codebases, generate proof-of-concept exploits, and orchestrate multi-stage intrusions that previously required teams of skilled human operators, compressing exploitation timelines from weeks to hours.[2]

At the same time, Indian courts have confronted a parallel wave of AI-enabled harm that sits at the intersection of cybersecurity and personal liberty: "digital arrest" frauds in which AI-assisted voice cloning and forged judicial documents are used to extort citizens, and a proliferating series of deepfake personality-rights suits before the Delhi and Bombay High

[1] Indian Computer Emergency Response Team (CERT-In), Blueprint for Reducing Exposure and Defending against AI-Assisted Vulnerabilities Exploitation in Digital Infrastructure, Version 1.0, Executive Summary & s. 14 (May 25, 2026)

[2] Indian Computer Emergency Response Team, *Defending Against Frontier AI Driven Cyber Risks*, Advisory No. CIAD-2026-0020 (Apr. 26, 2026)

Courts. The Supreme Court of India has itself taken suo motu cognizance of digital-arrest fraud and has issued directions concerning investigation, identification of mule bank accounts, and cooperation by relevant intermediaries and service providers.[3]

Against this backdrop of a technically sophisticated but formally non-binding regulatory response from the executive, an ad hoc, litigation-driven judicial response, and the absence of a targeted AIspecific amendment to the IT Act or an enacted Digital India Act, this project examines whether India's emerging cybersecurity framework is adequate to the threat it describes.

6. STATUTORY AND INSTITUTIONAL FRAMEWORK

Section 70B of the IT Act, inserted in 2009, empowers the Central Government to constitute CERT-In as the national nodal agency for cybersecurity, with functions spanning incident analysis, alerts, and the issuance of guidelines, advisories and directions. Section 70B(6) empowers CERT-In to issue binding directions to service providers, intermediaries, data centres and body corporates; Section 70B(7) penalises non-compliance with imprisonment of up to one year, a fine of up to ₹1 crore, or both — the fine ceiling having been raised from ₹1,00,000 by the Jan Vishwas (Amendment of Provisions) Act, 2023, with effect from 30 November 2023. Even at this increased level, the penalty remains a flat sum rather than the graduated, turnover-linked model Parliament has since adopted for data-protection failures under the DPDP Act.[4]

On 28 April 2022, CERT-In issued Directions under Section 70B(6) requiring mandatory reporting of specified cyber incidents including data breaches and attacks on IoT device within six hours of an entity noticing them, together with 180-day log retention and system time-synchronisation, a significant tightening of the "as early as possible" standard under the earlier CERT-In Rules, 2013.

This 2022 architecture remains the only source of binding, penalty-backed obligation in the

[3] *In re Victims of Digital Arrest Related to Forged Documents*, Suo Motu Writ Petition (Criminal) No. 3 of 2025 (Sup. Ct. India)

[4] Indian Computer Emergency Response Team, 'Roles and Functions' (cert-in.org.in); Information Technology (Amendment) Act, 2008, inserting ss 70A-70B w.e.f. 27 October 2009; Jan Vishwas (Amendment of Provisions) Act, 2023 (Act No. 18 of 2023), Schedule, item substituting 'one crore' for 'one lakh' in s 70B(7) of the IT Act, with effect from 30 November 2023.

field; the Blueprint does not displace it but merely reiterates the six-hour rule.[5]

Beyond CERT-In's coordination functions, the IT Act's substantive offence provisions retain independent relevance: Section 66C penalises identity theft through fraudulent use of another's unique identifying features, and Section 66D penalises cheating by personation using a computer resource provisions of obvious, if imperfect, relevance to AI-generated voice and video impersonation . Section 43A's residual civil-liability regime for failure to maintain reasonable security practices continue to apply alongside these criminal provisions, though it too predates any contemplation of AI-assisted attack.

The DPDP Act, 2023 introduces, for the first time, a general security-safeguard obligation (Section 8(5)) and a breach-notification duty (Section 8(6)), operationalised by the DPDP Rules, 2025 notified 13 November 2025 through a 72-hour notification window to the Data Protection Board.[6]

Critically, these substantive obligations do not commence until 13 May 2027; for the whole period examined here, CERT-In's instruments therefore operate without a contemporaneously enforceable general data-security statute, unlike the European Union, where the AI Act's cybersecurity requirements operate alongside an already fully-applicable GDPR.[7]

On 10 February 2026, MeitY amended the IT Rules to introduce specific obligations concerning synthetically generated information, including labelling and technical-provenance requirements, alongside revised and differentiated timelines for removal or disabling of access to specified unlawful content.[8]

Finally, India has deliberately avoided an umbrella AI statute: MeitY's India AI Governance Guidelines (5 November 2025) favour a "lightweight," sector-by-sector approach over EU-style horizontal regulation. It is this legislative vacuum that gives CERT-In's Blueprint its significance: everything CERT-In has said about AI-assisted threats has, to date, been said in

[5] Indian Computer Emergency Response Team (CERT-In), Directions Under Sub-Section (6) of Section 70B of the Information Technology Act, 2000, No. 20(3)/2022-CERT-In (Apr. 28, 2022), Direction (ii); Blueprint, *supra* note 1, s. 10.
[6] Digital Personal Data Protection Rules, 2025, G.S.R. 846(E), r. 7 (Nov. 13, 2025); Digital Personal Data Protection Act, 2023, No. 22 of 2023, s. 8(5)-(6) (India)
[7] Ministry of Electronics and Information Technology, Notification, G.S.R. 843(E) (Nov. 13, 2025); Digital Personal Data Protection Act, 2023, No. 22 of 2023, sch. (India)
[8] Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Amendment Rules, 2026, G.S.R. 120(E) (Feb. 10, 2026)

the register of guidance rather than law.[9]

7. CERT-IN'S AI-SPECIFIC FRAMEWORK

CERT-In's engagement with AI-specific cyber risk began with Advisory CIAD-2023-0015 on the security implications of language-model applications, followed on 26 March 2025 by CIAD-20250013, which catalogued attack techniques data poisoning, adversarial examples, prompt injection, model inversion and stealing and recommended user-facing precautions such as avoiding submission of sensitive data to public generative-AI tools. These early advisories were oriented principally toward AI as a tool to be used safely.[10]

That orientation shifted decisively with CIAD-2026-0020, issued 26 April 2026 and rated high severity. The advisory records that frontier AI systems demonstrate a "significant increase in cyber capability maturity" the ability autonomously to discover vulnerabilities across extensive codebases, generate proof-of-concept exploits, conduct automated reconnaissance, generate convincing multilingual phishing content, and plan multi-stage attacks involving privilege escalation and lateral movement. Its framing is explicitly dual-use: the same capability that aids defenders, the advisory notes, "could lower the barrier to entry for malicious cyber actors."[11]

Its recommendations are graduated by audience compressed patch timelines and zero-trust architecture for organisations, proportionate guidance for MSMEs, and, for individuals, heightened scepticism toward AI-generated voice and video communications, a direct response to the digital-arrest phenomenon discussed further.[12]

Notably, the advisory's evidentiary basis rests substantially on disclosures by foreign frontier-AI developers and the UK AI Security Institute's evaluations, rather than independent Indian technical assessment a point of significance .[13]

A month later, the Blueprint operationalised this threat assessment into a fourteen-section governance and technical-control framework addressing nine objectives, from reducing

[9] Ministry of Electronics and Information Technology, India AI Governance Guidelines (Nov. 5, 2025)
[10] Indian Computer Emergency Response Team (CERT-In), Advisory CIAD-2025-0013, Best Practices Against Vulnerabilities While Using Generative AI Solutions (Mar. 26, 2025), referencing Advisory CIAD-2023-0015, Security Implications of AI Language Based Applications (May 9, 2023)
[11] CIAD-2026-0020, *supra* note 2
[12] CIAD-2026-0020, *supra* note 2
[13] CIAD-2026-0020, *supra* note 2

exploitable exposure to strengthening executive accountability and coordinated threat-intelligence sharing with CERT-In, and setting out twelve "core defensive principles" assume breach, zero trust, defence-in-depth, continuous exposure management, secure-by-design, and others.[14]

It further introduces an "AI Bill of Materials" alongside the more familiar Software Bill of Materials, and a sixteen-point framework for "Secure Adoption and Governance of Artificial Intelligence Systems," including a distinct category for governing autonomous and agentic AI requiring defined operational boundaries, audit logging, and emergency-shutdown mechanisms. Ongoing assurance is anchored to CERT-In's own July 2025 Comprehensive Cyber Security Audit Policy Guidelines, which separately mandate annual third-party audits by CERT-In-empanelled auditors one of the few points at which the Blueprint's advisory content connects to an existing compliance obligation.[15]

Implementation is sequenced across a three-phase roadmap "Immediate Risk Reduction" (0-7 days), "Operational Strengthening" (8-30 days), and "Advanced Resilience and Adaptive Security" (31-60 days) signalling that CERT-In expects even voluntary adoption to proceed at a pace matched to the compressed threat timelines described in CIAD-2026-0020, rather than at the more leisurely cadence typical of prior guidance documents.[16]

Notwithstanding this technical sophistication, the Blueprint is explicit about its own non-binding character: organisations are "encouraged" to implement its recommendations "in a risk-informed manner based on operational criticality, threat exposure, and organisational maturity." Unlike the 2022 Directions, it does not recite Section 70B(6) as its source of authority and does not purport to be a "direction" it is better read as guidance issued under CERT-In's general advisory function.

This distinction, between the Blueprint's aspirational timelines and the 2022 Directions' binding six-hour rule, is the analytical hinge of this project.[17]

[14] *Supra* note 1, ss. 3, 5.
[15] *Supra* note 1, ss. 7, 12; Indian Computer Emergency Response Team (CERT-In), Comprehensive Cyber Security Audit Policy Guidelines (July 25, 2025)
[16] *Supra* note 1, s. 11
[17] *Supra* note 1, Executive Summary & s. 14.

8. JUDICIAL ENGAGEMENT WITH AI-ASSISTED CYBER THREATS

Judicial engagement with AI-assisted cyber harm builds on a pre-existing foundation. Justice K.S. Puttaswamy (Retd.) v. Union of India grounds the constitutional right to privacy in Article 21 and provides a broader constitutional foundation of dignity, autonomy and informational selfdetermination that can inform the protection of personality interests.[18]

Although decided in a data-protection context, Puttaswamy's recognition of informational selfdetermination as an incident of Article 21 has since supplied the doctrinal vocabulary dignity, autonomy, and control over one's own persona that High Courts now invoke when fashioning relief against non-consensual AI-generated depictions of real persons, discussed below.

Anvar P.V. v. P.K. Basheer and Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal require strict Section 65B certification for electronic evidence a continuing constraint as courts are increasingly called upon to authenticate or discredit synthetic audio-visual material. The current statutory framework is contained in Section 63 of the Bharatiya Sakshya Adhiniyam, 2023, which governs admissibility of electronic records. Shreya Singhal v. Union of India, which struck down Section 66A as unconstitutionally vague, counsels that any future deepfake-specific offence must be drafted with a precision Section 66A lacked.[19]

In the absence of codified deepfake law, High Courts have developed interim-injunction practice grounded in personality rights. In Rajat Sharma and Anr. v. Tamara Doc and Ors., the Delhi High Court restrained deepfake misuse of a journalist's name, likeness and voice, extending relief to "any existing or future technology such as Artificial Intelligence, deepfake technology," with a final decree fixing twenty-four and thirty-six hour platform-compliance windows and permitting the plaintiffs to report fresh URLs without returning to court.[20]

The most consequential intervention is the Supreme Court's suo motu proceeding, In Re: Victims of Digital Arrest Related to Forged Documents, initiated after a senior-citizen couple was defrauded of their life savings through a digital-arrest scam. Successive orders directed CBI-led investigation, identification of mule bank accounts, and cooperation from telecom

[18] Justice K.S. Puttaswamy (Retd.) v. Union of India, (2017) 10 SCC 1
[19] Anvar P.V. v. P.K. Basheer, (2014) 10 SCC 473; Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal, (2020) 7 SCC 1; Shreya Singhal v. Union of India, (2015) 5 SCC 1
[20] Rajat Sharma v. Tamara Doc, CS(COMM) 1147/2024 (Delhi H.C. Aug. 24, 2026)

providers and intermediaries.[21]

9. COMPARATIVE PERSPECTIVES

The European Union addresses AI-specific cybersecurity through Article 15 of the Artificial Intelligence Act, Regulation (EU) 2024/1689 a binding requirement that high-risk AI systems achieve an appropriate level of accuracy, robustness and cybersecurity, including resilience against adversarial manipulation and data or model poisoning.[22]

Compliance is enforced through conformity assessment and administrative fines of up to seven per cent of global turnover for the most serious infringements, with obligations for standalone highrisk systems applicable from 2 August 2026. Where CERT-In's twelve-hour patch timeline is framed within a document that disclaims binding force, the EU's comparable cybersecurity requirement is a conformity-assessed, fine-backed legal obligation operating alongside an already fully-applicable GDPR.[23]

The United Kingdom has proceeded through soft law, as India has, but with a clearer standardisation pathway. DSIT's Code of Practice for the Cyber Security of AI, published 31 January 2025, sets out thirteen lifecycle principles for developers, operators and data custodians; within months it was adopted by the European Telecommunications Standards Institute as global standard TS 104 223 converting domestic soft law into an internationally recognised baseline, a step CERT-In's Blueprint has not pursued.[24]

The United States framework is more fragmented but methodologically influential: NIST's draft Cybersecurity Framework Profile for Artificial Intelligence (NISTIR 8596, released December 2025) maps AI-specific considerations onto the pre-existing Cybersecurity Framework, while the Cybersecurity and Infrastructure Security Agency, the National Security Agency and the Federal Bureau of Investigation issued joint guidance on AI data security in May 2025. As in India, none of this US guidance carries independent statutory force suggesting CERT-In's choice of the advisory instrument is not, in itself, anomalous, even if, it remains

[21] In Re: Victims of Digital Arrest Related to Forged Documents, Suo Motu Writ Petition (Criminal) No. 3 of 2025, Order (Dec. 1, 2025) (Supreme Court of India)
[22] Regulation (EU) 2024/1689 (Artificial Intelligence Act), art. 15
[23] Regulation (EU) 2024/1689 (Artificial Intelligence Act), arts. 6(2), 15, 43–47, 99, Annex III, as amended by Regulation (EU) 2026/1744
[24] Department for Science, Innovation and Technology, Code of Practice for the Cyber Security of AI (Jan. 31, 2025)

inadequate to the scale of harm CERT-In itself has documented. Across all three jurisdictions, in short, the EU alone has chosen to make AI-specific cybersecurity a matter of directly enforceable law; the UK and the US, like India, rely on guidance but guidance that has, in the UK's case, achieved formal standards-body recognition CERT-In's Blueprint has not sought.[25]

10. ASSESSING THE ADEQUACY OF CERT-IN'S FRAMEWORK

CERT-In's framework has genuine strengths. It demonstrates institutional agility three escalating AI-specific instruments within roughly three years, tracking frontier-AI capability in close to real time. Its technical content is current, embedding zero-trust architecture, AIBOM-based supplychain visibility, and governance of agentic AI with defined shutdown mechanisms, placing it on a comparable technical footing with the EU, UK and US instruments examined in comparative perspective. And its twelve-hour patch timeline is, on the comparative evidence, more demanding than equivalent foreign benchmarks, suggesting CERT-In has not underestimated the threat's urgency.

The central structural weakness is the Blueprint's non-binding character. Because it does not recite Section 70B(6) and uses the language of encouragement rather than command, an organisation that ignores its recommendations commits no identifiable legal wrong under the Blueprint itself; liability, if any, must be reconstructed indirectly, through negligence or the DPDP Act's security safeguard obligation once it commences in May 2027. This is a materially weaker enforcement architecture than the EU's conformity-assessed obligation, and weaker even than the UK's, where voluntary adoption at least achieved the discipline of a formal ETSI standard.

Even where CERT-In's guidance connects to a binding obligation the 2022 Directions' six-hour reporting rule the applicable Section 70B(7) penalty, a flat sum raised by the Jan Vishwas Act, 2023 from ₹1,00,000 to a ceiling of ₹1 crore, is difficult to reconcile with the "cascading compromise" and national-security-level risks the Blueprint itself describes, and remains roughly 250-fold below the DPDP Act's ₹250 crore ceiling itself graduated by the nature, gravity and duration of the breach for a conceptually adjacent failure arising from the very

[25] National Institute of Standards and Technology, Cybersecurity Framework Profile for Artificial Intelligence (Cyber AI Profile), NISTIR 8596, Initial Preliminary Draft (Dec. 16, 2025); Cybersecurity and Infrastructure Security Agency, National Security Agency, & Federal Bureau of Investigation, Cybersecurity Information Sheet: AI Data Security (May 22, 2025)

same incident.[26]

Three further gaps compound this. First, a criminal-law gap: the Supreme Court's own finding, in the digital-arrest proceedings, that existing law does not squarely capture AI-assisted impersonation fraud at scale confirms that CERT-In's technical blueprint operates in isolation from the substantive criminal-law reform only Parliament can supply. Second, an open-source and agentic-AI blind spot: the Blueprint's supply-chain governance model presumes an identifiable commercial counterparty, with no clear application to open-weight models fine-tuned in-house, and its agentic-AI safeguards remain couched in the same non-binding register as the rest of the document at precisely the point where CERT-In's own threat assessment suggests risk is most acute. Third, an evaluation gap: CERT-In's most authoritative statement on frontier-AI cyber risk is, on its own citations, substantially import-dependent, absent an Indian equivalent of the UK's AI Security Institute.

Fourth, a resourcing gap: the Blueprint's tiered guidance for micro, small and medium enterprises is realistic in substance but unaccompanied by any subsidy, safe-harbour or grant mechanism, risking a widening compliance divide between well-resourced regulated entities and the broader digital economy CERT-In's own advisory now describes as effectively part of the frontline. Taken together, CERT-In has done the technical diagnostic work; the legislative and institutional response required to convert that diagnosis into enforceable regulation remains substantially outstanding.[27]

11. RECOMMENDATIONS

Five reforms would close the gaps identified above. First, the Blueprint's core timelines the twelvehour patch expectation for internet-facing crown-jewel systems in particular, presently indicative and applicable "where feasible" rather than mandatory should be reissued as formal Directions under Section 70B(6) for entities operating critical information infrastructure, so that noncompliance carries a legal consequence rather than none.

Second, Section 70B(7)'s flat ₹1 crore penalty ceiling raised from ₹1,00,000 by the Jan Vishwas Act, 2023, but still fixed regardless of an entity's size or the scale of harm caused

[26] Compare IT Act, s 70B(7), as amended by the Jan Vishwas (Amendment of Provisions) Act, 2023, with Schedule to the DPDP Act, 2023, entries against ss 8(5)-(6).
[27] CIAD-2026-0020, *supra* note 2, For Individuals

should be replaced with the DPDP Act's graduated, turnover-linked model, so that the consequence of ignoring a CERT-In direction concerning AI-assisted threats to critical systems scales with the harm at stake.

Third, the pending Digital India Act should be prioritised for introduction with a dedicated chapter creating a standalone offence for AI-assisted impersonation fraud, including "digital arrest" conduct, and a codified rather than purely judge-made right against non-consensual synthetic media, coordinated with the SGI labelling regime already in force under the 2026 IT Rules amendment.

Fourth, India should build independent frontier-model evaluation capacity whether within CERT-In or an allied body to reduce the evidentiary dependence on foreign disclosures that presently characterises its most authoritative AI-threat advisory.

Fifth, a subsidised empanelled-audit scheme or time-limited safe harbour should be introduced for MSMEs adopting a defined minimum subset of the Blueprint's recommendations, to prevent the resourcing gap identified above from widening as AI-assisted threats increasingly target smaller, less-resourced entities.

12. CONCLUSION

This project asked whether CERT-In's emerging cybersecurity framework is an adequate regulatory response to AI-assisted cyber threats in India. CERT-In's technical diagnosis is current and, in key respects, more demanding than comparable instruments issued by the EU, the UK and the US. What is missing is the legal architecture to match it: binding force for the Blueprint's core obligations, a penalty structure proportionate to the risks CERT-In itself describes, and on the Supreme Court's own reckoning in the digital-arrest proceedings a standalone criminal offence for

AI-assisted impersonation fraud. Until the Digital India Act, or a targeted amendment to the IT Act, supplies that architecture, India's response to AI-assisted cyber threats remains, in substance, a well-designed set of recommendations rather than a regulatory regime in the fuller sense achieved elsewhere. The gap is one of legal form, not technical understanding and Parliament, not CERTIn, is now best placed to close it.

BIBLIOGRAPHY

A. STATUTES AND DELEGATED LEGISLATION

1. The Constitution of India, art 21.

2. Information Technology Act, 2000, ss 43A, 66A (struck down), 66C, 66D,70A, 70B, 79.

3. Information Technology (Amendment) Act, 2008.

4. Jan Vishwas (Amendment of Provisions) Act, 2023 (Act No. 18 of 2023), Schedule (amending s 70B(7) of the IT Act, with effect from 30 November 2023).

5. Digital Personal Data Protection Act, 2023.

6. Digital Personal Data Protection Rules, 2025 (notified 13 November 2025).

7. Information Technology (Intermediary Guidelines and Digital Media Ethics Code)

   Amendment Rules, 2026, G.S.R. 120(E) dated 10 February 2026.

8. Digital India Act (proposed / draft not enacted as of September 2026).

B. CERT-IN INSTRUMENTS

1. No. 20(3)/2022-CERT-In, Directions under sub-section (6) of section 70B of the Information Technology Act, 2000 (28 April 2022).

2. Indian Computer Emergency Response Team, 'Roles and Functions' (cert-in.org.in).

3. CERT-In Advisory CIAD-2023-0015, Security implications of AI language based applications (2023).

4. CERT-In Advisory CIAD-2025-0013, Best Practices against vulnerabilities while using Generative AI solutions (26 March 2025).

5. CERT-In Advisory CIAD-2026-0020, Defending Against Frontier AI Driven Cyber Risks (26 April 2026).

6. CERT-In, Blueprint for Reducing Exposure and Defending against AI-Assisted Vulnerabilities Exploitation in Digital Infrastructure, Version 1.0 (25 May 2026).

7. CERT-In, Comprehensive Cyber Security Audit Policy Guidelines (July 2025).

C. TABLE OF CASES

1. Justice K.S. Puttaswamy (Retd.) v. Union of India, (2017) 10 SCC 1.

2. Shreya Singhal v. Union of India, (2015) 5 SCC 1.

3. Anvar P.V. v. P.K. Basheer & Ors., (2014) 10 SCC 473.

4. Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal, (2020) 7 SCC 1.

5. Rajat Sharma and Anr. v. Tamara Doc and Ors., CS(COMM) 1147/2024 (Delhi High Court).

6. *In Re*: Victims of Digital Arrest Related to Forged Documents, Suo Motu Writ Petition (Criminal) No. 3 of 2025 (Supreme Court of India).

D. FOREIGN AND COMPARATIVE INSTRUMENTS

1. Regulation (EU) 2024/1689 (Artificial Intelligence Act), arts 6, 9-15, 43-47, Annex III.

2. Regulation (EU) 2026/1744 (Digital Omnibus on AI), amending Regulation (EU) 2024/1689.

3. General Data Protection Regulation (EU) 2016/679.

4. UK Department for Science, Innovation and Technology, Code of Practice for the Cyber Security of AI (31 January 2025).

5. US National Institute of Standards and Technology, Cybersecurity Framework Profile for Artificial Intelligence (NISTIR 8596), Preliminary Draft (16 December 2025).

6. US Cybersecurity and Infrastructure Security Agency, National Security Agency and Federal Bureau of Investigation, Cybersecurity Information Sheet: AI Data Security (22 May 2025).

E. GOVERNMENT AND INSTITUTIONAL REPORTS

1. Ministry of Electronics and Information Technology, India AI Governance Guidelines (5 November 2025).

2. Ministry of Electronics and Information Technology, Notification bringing into force the DPDP Act and DPDP Rules in three phases (14 November 2025).