INDIAN JOURNAL OF LEGAL REVIEW

VOLUME 6 AND ISSUE 3 OF 2026

INSTITUTE OF LEGAL EDUCATION

INDIAN JOURNAL OF LEGAL REVIEW

APIS – 3920 – 0001 | ISSN - 2583-2344

(Open Access Journal)

Journal's Home Page – https://ijlr.iledu.in/

Journal's Editorial Page - https://ijlr.iledu.in/editorial-board/

Volume 6 and Issue 3 of 2026 (Access Full Issue on - https://ijlr.iledu.in/volume-6-and-issue-3-of-2026/)

Publisher

Prasanna S,

Chairman of Institute of Legal Education

No. 08, Arul Nagar, Seera Thoppu,

Maudhanda Kurichi, Srirangam,

Tiruchirappalli – 620102

Phone : +91 73059 14348 - info@iledu.in / Chairman@iledu.in

INDIAN JOURNAL OF LEGAL REVIEW [IJLR – IF SCORE – 7.58]

VOLUME 6 AND ISSUE 3 OF 2026

APIS – 3920 - 0001 *(and)* ISSN - 2583-2344

Published by

Institute of Legal Education

https://iledu.in

CYBER LAW AND CYBER CRIME IN INDIA: A COMPREHENSIVE LEGAL ANALYSIS

AUTHOR - ANKUR CHAUDHARY* & DR.JUHI SAXENA**

* STUDENT AT AMITY UNIVERSITY UTTAR PRADESH, LUCKNOW CAMPUS

** ASSISTANT PROFESSOR -II AT AMITY LAW SCHOOL, AMITY UNIVERSITY(U.P.) LUCKNOW CAMPUS

BEST CITATION - ANKUR CHAUDHARY & DR.JUHI SAXENA, CYBER LAW AND CYBER CRIME IN INDIA: A COMPREHENSIVE LEGAL ANALYSIS, *INDIAN JOURNAL OF LEGAL REVIEW (IJLR)*, 6 (3) OF 2026, PG. 876-883, APIS – 3920 – 0001 & ISSN - 2583-2344.

Abstract

India recorded 65,893 registered cyber crime cases during 2023, a figure that represents a 24.4 per cent increase over the preceding year and that law enforcement specialists regard as a significant undercount of true incidence. Against this backdrop, the adequacy of India's substantive legal framework for cyber crime takes on particular urgency. The primary statute governing cyber crime in India remains the Information Technology Act, 2000, a law drafted chiefly to facilitate e-commerce and digital governance rather than to address criminal conduct. Its criminal provisions were incorporated at a late stage and have required successive amendments to keep pace with the technology they were designed to regulate. The 2008 amendments, the three new criminal codes enacted in 2023, and the Digital Personal Data Protection Act of the same year have each added further layers without resolving the foundational problem: India does not have a coherent, purpose-designed cyber crime statute. The present paper examines whether the existing legislative architecture is adequate to the contemporary threat environment, how courts have interpreted its provisions, and what specific reforms are urgently needed to address these persistent gaps. The analysis draws on the doctrinal tradition established by Karnika Seth and Pavan Duggal, whose scholarship on the IT Act provides the foundational interpretive framework within which subsequent judicial and legislative developments must be understood. The paper proceeds through conceptual framework, legislative analysis, judicial interpretation, specific offence categories, institutional architecture, and comparative study before concluding with targeted recommendations for reform. Throughout, particular attention is paid to the interaction between criminal enforcement and constitutional rights, a tension that has defined Indian cyber law since the Supreme Court landmark decision in Shreya Singhal v. Union of India. The article, based on doctrinal and comparative research methodology, contributes to a better understanding of cyber crime governance in India and the direction in which legislative and institutional reforms must proceed to meet the demands of a rapidly evolving digital threat landscape.

Keywords: Cyber Crime; Information Technology Act, 2000; Judicial Interpretation; Digital Evidence; Constitutional Rights; Cyber Security; Comparative Law; Legislative Reform; Personal Data Protection; Intermediary Liability

1. Introduction

India recorded 65,893 registered cyber crime cases during 2023, a figure that represents a 24.4 per cent increase over the preceding year and that law enforcement specialists regard as a significant undercount of true incidence.[2014]

[2014] **National Crime Records Bureau,** *Crime in India 2022* (Ministry of Home Affairs, 2023) 14. The NCRB notes that actual incidence is likely three to four times higher than reported figures, given well-documented barriers to

INDIAN JOURNAL OF LEGAL REVIEW [IJLR – IF SCORE – 7.58]

VOLUME 6 AND ISSUE 3 OF 2026

APIS – 3920 - 0001 *(and)* ISSN - 2583-2344

Published by

Institute of Legal Education

https://iledu.in

The gap between recorded and actual cyber crime is not incidental. It reflects a structural problem in the relationship between citizens and investigative institutions, one rooted in technological unfamiliarity, scepticism about the utility of complaint registration, and the absence of accessible reporting channels in many districts. Against this backdrop, the adequacy of India's substantive legal framework for cyber crime takes on particular urgency.

The primary statute governing cyber crime in India remains the Information Technology Act, 2000, a law drafted chiefly to facilitate e-commerce and digital governance rather than to address criminal conduct.[2015] Its criminal provisions were incorporated at a late stage of drafting and have required successive amendments to keep pace with the technology they were designed to regulate. The 2008 amendments, the three new criminal codes enacted in 2023, and the Digital Personal Data Protection Act of the same year have each added further layers without resolving the foundational problem: India does not have a coherent, purpose-designed cyber crime statute. The present paper examines whether the existing legislative architecture is adequate to the contemporary threat environment, how courts have interpreted its provisions, and what specific reforms are needed.

The analysis draws on the doctrinal tradition established by Karnika Seth and Pavan Duggal, whose scholarship on the IT Act provides the foundational interpretive framework within which subsequent judicial and legislative developments must be understood.[2016] The paper proceeds through conceptual framework, legislative analysis, judicial interpretation, specific offence categories, institutional architecture, and comparative study before concluding with targeted recommendations for reform. Throughout, particular attention is paid to the interaction between criminal enforcement and constitutional rights, a tension that has defined Indian cyber law since the Supreme Court's landmark decision in *Shreya Singhal v. Union of India.*

2. Concept of Cyber Crime

No universally accepted statutory definition of cyber crime exists in Indian law, and the IT Act offers definitions of individual technical terms without characterising the criminal category as a whole. For the purposes of this paper, cyber crime is understood as any criminal offence in which a computer, computer network, or electronic device functions as the instrument, target, or repository of the conduct in question.[2017] This formulation, while broad, has the advantage of capturing three analytically distinct categories of conduct that each require somewhat different legal treatment.

Where a computer is the target of criminal conduct, the primary concern is with the integrity and confidentiality of digital systems: hacking, distributed denial-of-service attacks, the deployment of malware, and ransomware operations all fall within this category. Where a computer is an instrument, the crime is conventionally one that could theoretically occur without digital technology but that the technology facilitates at scale: phishing, identity theft, online fraud, and cyber stalking are examples. Where a computer serves as a repository, the device holds evidence of or proceeds from some other criminal activity rather than being implicated in the commission of the offence itself.[2018] This tripartite structure has direct implications for how investigative

complaint registration including technological unfamiliarity and police reluctance to record digital offences.

[2015] The IT Act was modelled on the UNCITRAL Model Law on Electronic Commerce (1996) and was primarily concerned with recognising electronic signatures, enabling e-governance, and facilitating digital contracting. Criminal provisions were included largely at the last stage of drafting and received far less legislative scrutiny than the civil and commercial provisions.

[2016] **Karnika Seth,** *Computers, Internet and New Technology Laws,* 2nd ed. (LexisNexis, 2016) 12. Seth's analysis remains the most systematic treatment of the IT Act's criminal provisions from an Indian doctrinal perspective.

[2017] The working definition adopted here is broadly consistent with the approach taken in the Council of Europe's Budapest Convention explanatory report (para. 35–37), which similarly refuses a single statutory definition in favour of a conduct-based taxonomy.

[2018] **David S. Wall,** *Cybercrime: The Transformation of Crime in the Information Age* (Polity Press, 2007) 7. Wall's tripartite taxonomy has been widely adopted in subsequent scholarship and informs several national legislative frameworks.

INDIAN JOURNAL OF LEGAL REVIEW [IJLR – IF SCORE – 7.58]
VOLUME 6 AND ISSUE 3 OF 2026
APIS – 3920 - 0001 *(and)* ISSN - 2583-2344
Published by
Institute of Legal Education
https://iledu.in

powers should be calibrated and how jurisdiction should be allocated across state and central agencies.

The economic consequences of cyber crime in India, though difficult to quantify precisely, are substantial by any measure. Industry estimates consistently place annual losses above Rs 1.7 lakh crore when direct financial fraud, ransomware payments, intellectual property theft, and remediation costs are aggregated. The personal harm visited on victims of cyber stalking, non-consensual intimate imagery, and identity fraud is harder to capture in a single figure but shapes the urgency of legislative reform just as powerfully as any macroeconomic estimate.

3. The Legislative Framework

The IT Act's criminal architecture was significantly expanded by the 2008 Amendment, which introduced the cyber terrorism provision under Section 66F, the privacy violation offence under Section 66E, and a suite of identity-related offences across Sections 66B through 66D. Parliament also added Section 66A, which criminalised electronic communication deemed to be grossly offensive, menacing, or persistently annoying. That provision attracted increasing criticism from civil liberties scholars even before a series of high-profile arrests brought it to national attention.[2019] The constitutional vulnerability that commentators had identified from the outset was ultimately confirmed by the Supreme Court in 2015, a development examined in the judicial section below.

The most practically significant provision for general computer misuse is Section 66, which creates an offence for anyone who commits an act referred to in Section 43 with the knowledge or intention that wrongful loss or damage to any person will result, and which carries a maximum term of three years' imprisonment and a fine of up to five lakh rupees. The cross-reference to Section 43, a civil liability provision, has generated considerable interpretive difficulty: prosecutors must simultaneously engage with civil and criminal standards, and courts have had to develop ad hoc approaches to the resulting ambiguity.[2020] The maximum sentence, which appeared proportionate in the context of relatively low-scale intrusions in 2000, is now widely regarded as inadequate given the scale of harm that sophisticated cyber attacks can cause.

The Bharatiya Sakshya Adhiniyam, 2023 represents the most practically important development in the legal treatment of digital evidence since the IT Act itself. By restructuring the admissibility regime for electronic records, the BSA substantially addresses the bottleneck created by the Section 65B certificate requirement, which had been the subject of prolonged and contentious litigation culminating in the Supreme Court's decision in *Arjun Panditrao Khotkar*.[2021] Whether the revised framework will achieve its intended simplification in practice depends heavily on how trial courts apply it in the years ahead, and early indications from high courts suggest that interpretive disputes will continue for some time.

The CERT-In Directions issued in April 2022 occupy an important and contested position in the regulatory architecture. By imposing mandatory incident reporting obligations on a broad category of entities and requiring extensive log retention, the Directions significantly expand the state's capacity for cyber security oversight.[2022] At the same time,

[2019] **Parliament of India,** *Report of the Standing Committee on Information Technology on the Information Technology (Amendment) Bill 2006* (Lok Sabha Secretariat, 2007) 22–24. The Committee expressed concern about the breadth of the proposed amendments but did not specifically address what became Section 66A.

[2020] **Pavan Duggal,** *Cyberlaw: The Indian Perspective*, 4th ed. (Saakshar Law Publications, 2020) 189. Duggal was among the first Indian commentators to identify the constitutional vulnerability of Section 66A following the 2012 arrests of the two Mumbai women.

[2021] *Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal* (2020) 7 SCC 1, paras 18–22. The Court held that the certificate must come from the person responsible for the computer system at the time the record was generated or stored, not merely at the time of production in court.

[2022] The CERT-In Directions of 28 April 2022 imposed mandatory incident reporting within six hours for sixty-one categories of entities, retention of logs for 180 days, clock synchronisation with NTP servers, and a requirement that VPN service providers retain user data including subscriber names, IP

INDIAN JOURNAL OF LEGAL REVIEW [IJLR – IF SCORE – 7.58]
VOLUME 6 AND ISSUE 3 OF 2026
APIS – 3920 - 0001 *(and)* ISSN - 2583-2344
Published by
Institute of Legal Education
https://iledu.in

several of the requirements have been challenged as disproportionate under the privacy framework established in *Puttaswamy,* particularly the requirement that VPN service providers maintain detailed subscriber records. These challenges have not yet been finally resolved, leaving a significant portion of the subordinate legislative framework in a state of constitutional uncertainty.

4. Judicial Interpretation of Cyber Crime Provisions

Shreya Singhal v. Union of India decided in 2015 by a two-judge bench of the Supreme Court stands as the most far-reaching judicial pronouncement on the scope and limits of Indian cyber law. The Court struck down Section 66A in its entirety, holding that the provision failed every constitutional test applicable to restrictions on speech: it was vague in its terms, overbroad in its reach, and could not be brought within the categories of permissible restriction under Article 19(2) of the Constitution.[2023] The judgment is notable not only for its immediate holding but for its elaboration of a framework for evaluating the constitutional validity of cyber crime provisions that has been applied repeatedly in subsequent litigation.

On the question of intermediary liability under Section 79, the Court upheld the provision but read it down to require that an intermediary loses its immunity only where it fails to act upon actual knowledge of unlawful content brought to its attention by a court order or a government notification, not by a private complaint.[2024] This interpretation has had substantial practical consequences for the manner in which platforms respond to content removal requests, and it has been the subject of ongoing regulatory tension as the government has sought through the 2021 Intermediary Rules to shift the threshold for required action.

K.S. Puttaswamy v. Union of India, decided in 2017 by a nine-judge bench, established the right to privacy as a fundamental right protected under the Constitution and articulated a four-part proportionality framework that governs all state interference with that right.[2025] The judgment's implications for cyber law are pervasive. Surveillance powers under Sections 69 and 69B of the IT Act, content blocking under Section 69A, mandatory data retention under the CERT-In Directions, and the DPDP Act's framework for government data access must all be assessed against the *Puttaswamy* proportionality standard. No comprehensive judicial review of these provisions has yet occurred, and the gap between the constitutional standard and the legislative framework is a source of ongoing litigation.

5. Analysis of Specific Cyber Crime Categories

5.1 Ransomware and Critical Infrastructure Attacks

The AIIMS Delhi ransomware attack of November 2022 provides the sharpest illustration of the gap between the sophistication of contemporary cyber crime and the adequacy of the existing statutory framework. The attack disabled the hospital's digital infrastructure for approximately two weeks, potentially exposing the health records of millions of patients.[2026] When investigators sought to prosecute the perpetrators, they found no dedicated ransomware provision in Indian law. The case had to be constructed from Section 66 of the IT Act, the extortion provision in the BNS, and money laundering

addresses, and usage logs for five years. Several VPN providers exited the Indian market in response.

[2023] *Shreya Singhal v. Union of India* (2015) 5 SCC 1, para. 47. The Court drew on First Amendment jurisprudence from the United States, particularly *Reno v. ACLU* (1997), in characterising the internet as a unique medium deserving the highest protection.

[2024] *Ibid.,* para. 52–58. The advocacy/incitement distinction had been articulated in *Ramji Lal Modi v. State of U.P.* AIR 1957 SC 620, which the *Shreya Singhal* bench applied to the online context.

[2025] *K.S. Puttaswamy v. Union of India* (2017) 10 SCC 1, para. 267 (Chandrachud J., concurring). The proportionality framework requires: (i) a law; (ii) a legitimate state aim; (iii) proportionality between the means and the aim; and (iv) procedural guarantees. All four limbs must be satisfied for any invasion of privacy.

[2026] **Ministry of Home Affairs,** *Annual Report on Cyber Crime in India* (Government of India, 2023) 22. The report details the AIIMS investigation, noting that data from approximately 1.3 crore patients was potentially compromised, including medical histories and test results.

INDIAN JOURNAL OF LEGAL REVIEW [IJLR – IF SCORE – 7.58]
VOLUME 6 AND ISSUE 3 OF 2026
APIS – 3920 - 0001 *(and)* ISSN - 2583-2344
Published by
Institute of Legal Education
https://iledu.in

legislation, each requiring independent proof of distinct elements, and each carrying penalties that bore little relationship to the severity of the harm caused.[2027]

5.2 Deepfakes and Synthetic Media

Deepfakes present a distinct legislative challenge because the harm they cause is not adequately captured by any existing provision. Where a deepfake is used to defame, Section 356 BNS provides some remedy, but defamation law does not address the distribution of non-consensual intimate imagery. Where it is used to defraud, the fraud provisions of the BNS may apply, but the dignity harm to the subject of the deepfake is beyond the reach of a fraud charge. Section 66E of the IT Act covers violation of privacy through capturing or transmitting an intimate image, but it requires that the original image was captured in a private context, a condition that synthetic media by definition does not satisfy.[2028] The result is that one of the most rapidly growing categories of gender-based cyber crime sits in a legislative void.

5.3 Cyber Terrorism

Cyber terrorism under Section 66F illustrates a different problem: the provision is drafted with sufficient breadth that its limits are unclear, and the absence of any concluded prosecution means that those limits have never been tested judicially. The maximum punishment of life imprisonment makes the definitional uncertainty particularly consequential, since the difference between a criminal hacker and a cyber terrorist under the current statutory text may turn on prosecutorial discretion rather than any principled legal distinction. Security researchers, ethical hackers, and journalists who expose digital vulnerabilities all occupy legally precarious ground under a provision whose outer boundary has never been authoritatively defined.

6. The Institutional Architecture

India's institutional framework for cyber crime response is distributed across several agencies without a clear command hierarchy. CERT-In holds statutory responsibility for cyber security incident response under Section 70B of the IT Act; NCIIPC protects designated critical information infrastructure; and I4C, operating under the Ministry of Home Affairs, coordinates the investigative work of state police cyber cells through the national reporting portal. The portal has processed a substantial volume of complaints since its 2019 launch, but the conversion rate from complaint to formal FIR registration remains very low.[2029] This gap reflects systemic failures at the investigation stage rather than a shortage of victim reporting.

A Parliamentary Standing Committee review conducted in 2023 found that twenty-eight of thirty-six states and union territories lacked dedicated cyber forensic laboratories.[2030] The implications of this finding extend beyond the immediate evidentiary consequences. When digital evidence cannot be examined locally, it must be sent to central facilities, creating delays that frequently exceed the period within which volatile evidence can usefully be retrieved or preserved. The problem is compounded by a shortage of prosecutors with sufficient technical training to present digital evidence effectively in court, and by a judiciary that frequently requires expert witnesses to establish propositions that are routine in jurisdictions with greater institutional investment in digital literacy across the criminal justice system.

[2027] The legislative gap on ransomware is widely recognised. A 2023 discussion paper by the Cyber Law Research Unit at NALSAR University of Law identified at least nine separate provisions across the IT Act, BNS, Prevention of Money Laundering Act 2002, and Foreign Exchange Management Act 1999 that might apply to a sophisticated ransomware attack, with no single provision covering the full conduct.

[2028] **Pavan Duggal,** *Cyberlaw: The Indian Perspective,* 4th ed. (Saakshar Law Publications, 2020) 212. Duggal identifies the synthetic-media gap as among the most pressing legislative challenges, noting that Section 66E was drafted with physical camera capture in mind rather than AI-generated imagery.

[2029] Duggal 245. The complaint-to-FIR conversion rate is itself disputed: cyber crime cells in several states have been found to classify complaints as 'resolved' after informal mediation with the accused, without registering an FIR, which inflates apparent resolution statistics.

[2030] **Parliamentary Standing Committee on Finance,** *The Digital Personal Data Protection Bill 2023* (Lok Sabha Secretariat, 2023) 34 and 41. The Committee found that seventeen states had no dedicated cyber crime investigation unit at the district level.

INDIAN JOURNAL OF LEGAL REVIEW [IJLR – IF SCORE – 7.58]

VOLUME 6 AND ISSUE 3 OF 2026

APIS – 3920 - 0001 *(and)* ISSN - 2583-2344

Published by

Institute of Legal Education

https://iledu.in

7. Comparative Analysis: Selected International Frameworks

The European Union's NIS2 Directive, which came into force in January 2023, illustrates the direction in which advanced jurisdictions are moving on critical infrastructure cyber security. The Directive imposes mandatory security obligations on entities across eighteen sectors, calibrates reporting timelines to the severity of the incident, and creates board-level personal liability for compliance failures.[2031] The requirement of a preliminary notification within twenty-four hours and a comprehensive report within seventy-two hours is particularly instructive for the Indian context, where the CERT-In Directions impose a six-hour reporting window across a very broad category of entities, a requirement so demanding that compliance has been uneven and the chilling effect on incident disclosure has been the subject of policy criticism.

The United Kingdom Computer Misuse Act, 1990 demonstrates the value of a structured, tiered approach to cyber crime legislation that can accommodate technological change through targeted amendment rather than wholesale replacement. Its three-tier offence structure, calibrated to the degree of authorisation and the severity of the resulting harm, provides courts with a framework for proportionate sentencing that the flat structure of Section 66 of the IT Act does not.[2032] The addition in 2015 of a life imprisonment provision for attacks on critical infrastructure shows that the tiered approach does not preclude severe penalties where they are warranted; it simply ensures that proportionality between the offence and the response is built into the statutory framework from the outset.

The Budapest Convention on Cybercrime remains the most important international reference point for any assessment of India's position in the global cyber crime enforcement landscape. Its procedural framework for cross-border evidence preservation and its twenty-four-hour emergency network for mutual assistance requests address precisely the bottlenecks that most severely hamper Indian investigators dealing with overseas-hosted evidence.[2033] India's decision not to accede to the Convention has repeatedly been defended on sovereignty grounds, but the practical cost of non-participation is borne almost entirely by domestic investigators and victims rather than by the state interests that the sovereignty argument is designed to protect.

8. Critical Assessment

Five structural deficiencies collectively define the inadequacy of India's current cyber crime framework. The first is a mismatch between the statutory text and the contemporary threat environment. Ransomware, deepfakes, synthetic fraud enabled by large language models, and attacks on Internet of Things devices were not within the contemplation of the IT Act's drafters, and the existing provisions cannot be stretched to address them without creating interpretive distortions that undermine legal certainty.[2034] The second deficiency is in penalty calibration: the sentencing framework does not adequately reflect the potential severity of harm, creating a deterrence gap that sophisticated criminal actors can rationally exploit.

The third deficiency concerns evidence. Despite the BSA's reforms, the challenges of obtaining cloud-hosted evidence from overseas providers

[2031] European Parliament, Directive (EU) 2022/2555 (NIS2 Directive), Art. 21 and Recital 79. The NIS2 framework distinguishes between 'essential entities' (which face more stringent obligations and proactive supervision) and 'important entities' (which face compliance-based oversight), calibrating the regulatory burden to the criticality of the sector.

[2032] **Ian Walden,** *Computer Crimes and Digital Investigations,* 2nd ed. (Oxford University Press, 2016) 203. Walden traces the CMA's evolution through four amendments and identifies the 2015 Act's Section 3ZA as the most significant expansion, noting that its 'serious damage' threshold mirrors the Budapest Convention's critical infrastructure provisions.

[2033] **Council of Europe,** *Explanatory Report to the Budapest Convention on Cybercrime,* ETS No. 185 (2001) para. 234. The 24/7 Network has handled over 3,000 emergency requests annually in recent years, with average response times of under two hours for expedited preservation requests, a speed that is structurally unavailable through standard MLAT channels.

[2034] Seth 201. Seth identifies six categories of penalty misalignment in the IT Act, noting that the maximum three-year sentence under Section 66 compares unfavourably with the maximum ten years under the UK Computer Misuse Act for similar conduct and the CFAA's provision for up to twenty years for aggravated offences.

INDIAN JOURNAL OF LEGAL REVIEW [IJLR – IF SCORE – 7.58]
VOLUME 6 AND ISSUE 3 OF 2026
APIS – 3920 - 0001 *(and)* ISSN - 2583-2344
Published by
Institute of Legal Education
https://iledu.in

and of authenticating communications encrypted end-to-end remain significant. The fourth is institutional: the distributed architecture of cyber crime investigation, without a genuine command structure or mandatory coordination mechanisms, results in duplication of effort, jurisdictional disputes, and inconsistent enforcement standards across state borders. The fifth is international: India's non-participation in the Budapest Convention framework and its absence of dedicated data access agreements with major cloud-hosting jurisdictions means that digital evidence is routinely unavailable or arrives too late to be useful.[2035]

9. Suggestions and Recommendations

The most important single reform would be the enactment of a comprehensive Cyber Security and Cyber Crime Act that consolidates the relevant provisions of the IT Act, the BNS, and related legislation into a single, purpose-designed statute with a tiered offence structure, penalties calibrated to actual harm, and specific provisions for ransomware, deepfakes, and attacks on critical infrastructure. Such a statute would also provide the occasion for placing the CERT-In Directions on a proper statutory footing and building the judicial oversight requirements that the *Puttaswamy* framework demands into the legislation itself.[2036]

India's accession to the Budapest Convention should follow as a matter of priority. The sovereignty concerns that have hitherto prevented accession are not groundless, but they must be weighed against the concrete operational costs of non-participation, which fall on domestic investigators and their ability to secure evidence in cross-border cases. Bilateral data access agreements modelled on the US CLOUD Act framework would complement Convention accession by providing expedited, legally certain mechanisms for evidence requests directed at the major cloud service providers.[2037]

On the institutional side, the most urgent priority is investment in forensic laboratory capacity across all states, accompanied by accreditation standards that ensure the admissibility of forensic evidence produced by those laboratories. A unified cyber crime command structure under I4C, with genuine authority to coordinate federal and state investigations and to standardise forensic protocols, would address the institutional fragmentation that has produced the very low prosecution conversion rates documented by Parliamentary oversight committees. A dedicated compensation fund for victims of cyber financial fraud, financed through levies on digital payment service providers, would address the harm gap that exists even where prosecution is ultimately successful.

10. Conclusion

India's cyber crime legal framework is characterised by a persistent gap between legislative aspiration and enforcement reality. The IT Act and its successor instruments articulate a broad set of criminal prohibitions, but the investigative, prosecutorial, and judicial infrastructure needed to give those prohibitions practical effect has not been developed at anything like the same pace. The decisions in *Shreya Singhal* and *Puttaswamy* have performed the important function of establishing constitutional limits on the framework, ensuring that the expansion of criminal liability cannot come at the unlimited expense of civil liberties. But constitutional constraint is not the same as legislative

[2035] Duggal 245. The distributed institutional architecture has also been criticised in the Comptroller and Auditor General of India's 2022 report on cyber security preparedness, which identified coordination failures between CERT-In and state-level investigating agencies as a primary driver of poor enforcement outcomes.

[2036] *Puttaswamy* para. 271–275 (Kaul J., concurring). Justice Kaul's concurrence is particularly instructive on data retention mandates, holding that any obligation to retain personal data beyond operational necessity requires specific statutory authorisation and judicial oversight.

[2037] **UNODC,** *Comprehensive Study on Cybercrime* (United Nations Office on Drugs and Crime, 2013) 67. The study found that countries with ratified mutual legal assistance treaties processed digital evidence requests in an average of 14 months, compared to 26 months for requests made through diplomatic channels alone.

adequacy, and the two must be pursued simultaneously.

Seth's observation that the effectiveness of cyber law ultimately depends on the capacity of institutions to implement it and the willingness of the state to invest in that capacity captures the essential challenge.[2038] Legislative reform of the kind recommended in this paper is necessary but not sufficient. It must be accompanied by sustained investment in forensic infrastructure, prosecutorial training, judicial education, and international cooperation mechanisms. Without that investment, even the best-drafted statute will produce the same pattern of underenforcement that characterises the current framework. The scale of the problem India faces, measured both in the economic cost of cyber crime and in the personal harm it inflicts, makes that investment not an optional enhancement but a fundamental obligation of the state.

References

1. **Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal.** (2020) 7 SCC 1. Supreme Court of India.
2. **Council of Europe. Convention on Cybercrime (Budapest Convention),** ETS No. 185. Council of Europe, 2001.
3. **Council of Europe. Explanatory Report to the Convention on Cybercrime.** Council of Europe, 2001.
4. **Duggal, Pavan. Cyberlaw: The Indian Perspective.** 4th ed., Saakshar Law Publications, 2020.
5. **European Parliament.** Directive (EU) 2022/2555 on Measures for a High Common Level of Cybersecurity across the Union (NIS2 Directive). **Official Journal of the European Union,** 2022.
6. **K.S. Puttaswamy v. Union of India.** (2017) 10 SCC 1. Supreme Court of India.
7. **Ministry of Home Affairs. Annual Report on Cyber Crime in India.** Government of India, 2023.
8. **National Crime Records Bureau. Crime in India 2022.** Ministry of Home Affairs, Government of India, 2023.
9. **Parliamentary Standing Committee on Finance. The Digital Personal Data Protection Bill 2023.** Lok Sabha Secretariat, 2023.
10. **Seth, Karnika. Computers, Internet and New Technology Laws.** 2nd ed., LexisNexis, 2016.
11. **Shreya Singhal v. Union of India.** (2015) 5 SCC 1. Supreme Court of India.
12. **UNODC. Comprehensive Study on Cybercrime.** United Nations Office on Drugs and Crime, 2013.
13. **Walden, Ian. Computer Crimes and Digital Investigations.** 2nd ed., Oxford University Press, 2016.
14. **Wall, David S. Cybercrime: The Transformation of Crime in the Information Age.** Polity Press, 2007.

[2038]Seth 312. The observation reflects a recurring theme in Seth's work: that India has generally enacted cyber crime legislation adequate in its stated scope but deficient in implementation capacity, creating a substantial gap between formal legal norms and on-the-ground enforcement.