INTERNATIONAL JOURNAL FOR LEGAL RESEARCH AND ANALYSIS

ISSN: 2582-6433

November 2026

RESEARCH ARTICLE

Cybercrime Enforcement In India: Legal And Institutional Barriers And Regional Disparities

Pavithra P

SASTRA Deemed University

www.ijlra.com

ABOUT THE JOURNAL

International Journal for Legal Research and Analysis (IJLRA)

ISSN: 2582-6433

IJLRA provides a platform for scholarly writing and discussion on law, legal research and interdisciplinary questions. Research articles explore legal principles, institutions, policy and contemporary developments.

Journal website: www.ijlra.com

PUBLICATION INFORMATION

International Journal for Legal Research and Analysis

ISSN: 2582-6433

Editorial note

The views and arguments expressed in this article are those of its author(s). Readers should consult the original legal authorities and sources cited in the manuscript.

Copyright and permissions are subject to the applicable publication agreement.

ARTICLE DETAILS

Cybercrime Enforcement In India: Legal And Institutional Barriers And Regional Disparities

Author: Pavithra P

Institution: SASTRA Deemed University

Journal: International Journal for Legal Research and Analysis

ISSN: 2582-6433

Cybercrime Enforcement In India: Legal And Institutional Barriers And Regional Disparities

Pavithra P

SASTRA Deemed University

ABSTRACT

India's digital economy has grown faster than the machinery meant to police it. Recorder cyber crime arose from 44,735 cases in 2019 86, 420 in 2023, yet in 2023 only about one in five cyber fraud cases reached a charge sheet stage and just 22 enter in conviction. This paper adopts doctrinal methodology and analysis of Information technology Act 2000, Bhartiya Nyaya Sanhita 2023, the Bharatiya Nagarik Suraksha Sanhita 2023, and Bhartiya Sakshya Adhiniyam 2023, read with leading judgments and official data placed before parliament, to examine the legal and procedural barriers to investigation and prosecution, the institutional architecture built by the union and states and regional disparities in enforcement outcomes.

The paper argues that section 78 of the IT act fixes investigative competence by rank rather than by technical skill, that this rule combined with uneven forensic capacity, jurisdictional fragmentation an informal complaint handling practice, leaves victims in many district without an effective first response and that the passive gap in statutory definitions is better understood as a gap in offense mapping and training than as an absence of law. As an original contribution the paper bills to analytical tools from official 2023 data and that do not appear in the literature reviewed: and enforcement attrition funnel, which shows that larger loss occurs after the charge sheet stage rather than before it, and capacity outcome typology of states, which Shows that regional disparities at least 3 distinct phenomena(overload, a possible small base effect and data classification failure in the highest volume state) rather than one. The paper suggest a competence based amendment to section 78, statutory timelines for converting portal complaints into FIRs, a national offense mapping protocol for emerging modus operandi, an equalisation of forensic and prosecutorial capacity, differentiated by which of these causes is actually operating in a given state.

Keywords: Cybercrime, information technology Act, section 78, mapping protocol, complaints.

TABLE OF CONTENTS

CHAPTER1:INTRODUCTION

1. Background and significance of the research area

2. Literature Review

3. Statement of the Research Problem

4. Research objectives

5. Research questions

6. Scope and limitations

7. Structure of the paper

CHAPTER 11: MAIN BODY

2.1. Research Methodology

2.2. findings

2.2.1. The existing legal framework (RQ1)

2.2.2.Legal and procedural barriers(RQ2)

2.2.3 The institutional framework(RQ3)

2.2.4 Regional disparities(RQ4)

2.2.5 Jurisdictional fragmentation as a barrier distinct capacity(RQ2/RQ4)

2.3 Discussion(RQ5)

2.4 An analytical contribution

2.4.1. The enforcement attrition funnel

2.4.2 A capacity outcome typology of states

CHAPTER 111: CONCLUSION

CHAPTER 1V:SUGGESTIONS AND FUTURE DIRECTIONS

4.1.Suggestions

4.2. Future Directions

CHAPTER V: REFERENCES

APPENDIX

CHAPTER 1: INTRODUCTION

1.1.Background and significance of the Research Area

Cybercrime has moved from margins of policing to its centre. Data complied by the national Crime Records Bureau (NCRB) and placed before parliament show that registered cybercrime almost doubled between 2019 and 2023 from 44,735 to 86420 cases.[1] The nature of offending has changed as well. Fraud and cheating together made up 36409 of the 86420 cases in 2023 and organised digital arrest scams in which offenders pose an investigators or judges over a video calls, led the Supreme court to take a Suo motto cognisance in October 2025.[2]

Enforcement however state responsibility. Police and public order fall in the state list, and the Union supplements state effort through advisories and funding. Whether a victim receives a meaning full response therefore depends on three things: how the statue allocate investigative authority, how state police apply those provisions at front desk, and what forensic and prosecutorial capacity exists in the district. The subject matters because an effective remedy is part of the promise of equal protection of the law, and because public trust in digital transactions depends on visible enforcement.

1.2. Literature Review

Five strands of peer reviewed scholarship inform this study. Kshetri states Indian cybercrime in developmental and institutional status which establish low rates of reporting, prosecution, and conviction connected with limited capacity.

. [3]Kethineni offers a descriptive survey of legislation, law enforcement structure and enforcement mechanism governing cybercrime in India, though it pre-dates the 2023 criminal codes .[4]Elavarasi and Elango identify the scarcity of technicality trained police officers and jurisdictional difficulty as central weakness and call for more cyber police stations and forensic laboratories. and also examine the challenges of Handling the electronic evidences and digital forensic in criminal investigation. [5]Banu and Banerjee points out that there is a lag in standardised forensic procedure in India.

---

[1] :
[1] Ministry of Home Affairs (MHA), Lok Sabha Unstarred Question No 452 (answered 2 December 2025), Annexures I–II (NCRB, 'Crime in India' data). https://www.mha.gov.in/MHA1/Par2017/pdfs/par2025-pdfs/LS02122025/452.pdf

[2] In re Victims of Digital Arrest Related to Forged Documents (Supreme Court of India, suo motu proceedings initiated 17 October 2025); 'SC Takes Strong Note of Rising Digital Arrest Scams, Seeks Centre and CBI Response' (All India Radio News, 17 October 2025).https://www.newsonair.gov.in/sc-takes-strong-note-of-rising-digital-arrest-scams-seeks-centre-and-cbi-response

[3] Nir Kshetri, 'Cybercrime and Cybersecurity in India: Causes, Consequences and Implications for the Future' (2016) 66 Crime, Law and Social Change 313https://www.newsonair.gov.in/sc-takes-strong-note-of-rising-digital-arrest-scams-seeks-centre-and-cbi-response

[4] Elavarasi and Elango, 'Analysis of Cybercrime Investigation Mechanism in India' (2020) Indian Journal of Science and Technology.
https://indjst.org/articles/analysis-of-cybercrime-investigation-mechanism-in-india

[5] A Banu R and J Banerjee, 'Examining the Role of Digital Forensics in Strengthening Cybercrime Investigations in India' (2025) 4(1) International Journal of Human Rights Law Review 60.
https://humanrightlawreview.in/wp-content/uploads/2026/02/Examining-the-Role-of-Digital-Forensics-in-Strengthening-Cybercrime-Investigations-in-India.pdf

These work establish the capacity is thin and evidence handling is difficult what they do not do is examine hoe the rank based investigative rule is 78 of the IT Act interacts with front desk practice under the new procedural code or analyse state wise enforcement outcomes using the head wise data now available. This paper addresses the gap.

1.3 Statement of the Research Problem

Cyber crime reporting is rising, but conversion of complaints into investigations, chargesheets and convictions is weak and uneven across states. Section 78 of the IT Act confines investigation of offences under that Act to officers of inspectors rank or above without any requirement of technical competence. Complainants in many districts are reportedly told that the officer at the station cannot investigate, and emerging modus operandi that the statues do not name are often recorded under generic heads or not pursued. The problem is whether the existing legal and institutional framework equips the state to investigate and prosecute cyber crime effectively and equitably across regions.

1.4.Research objectives

1.To map the legal framework governing investigation and prosecution of cyber crime in India.

2. To identify legal and procedural barriers with particular attention to section 78 of IT act and front desk refusal.

3.To evaluate the institutional framework for prevention, investigation and prosecution.

4. To assess institutional and infrastructural factors relevant to regional disparities and to propose reforms.

1.5 Research questions

1. What is existing legal framework governing the governing the investigation and prosecution of cyber crime in India?

2. What are the legal and institutional obstacles exist in the current framework regard to investigation and prosecution aspects?

3. How does the institution framework facilitate prevention investigation and prosecution?

4. What are the institutional and structural factors drive regional variations in regulatory compliance and enforcement?

5. .How effectively does current legal and institutional framework mitigate these enforcement challenges?

1.6 Scope and Limitation

The study covers the IT Act 2000 the BNS, BNSS and BSA 2023 constitutional prevention on policing and institutional arrangements of the ministry of Home Affairs under states using case law and official data up to September 2026. It does not undertake comparative analysis and it treats cyber security regulation and data protection law only, where they bear on enforcement. The methodology is entirely doctrinal it works from statues judgments and published government records and does not involve any survey interview or field visit. Three limitations follow from this

choice first NCRB figures measure registration not incidence the government itself states that NCRB does not maintain data on the share of victims who report[6]. Second, No public data give state wise numbers of cyber train inspectors so capacity is inferred from infrastructure indicators rather than measure directly. Third, because the analysis is doctrinal and documentary rather than empirical it can identify association and pattern in the published data but cannot establish causation, conclusion, about why outcomes differ across state are offered as the most plausible reading of the legal and documentary record, not as tested empirical findings.

1.7 Structure of the Paper

Chapter 2 sets of the methodology findings and discussion chapter 3 concludes. Chapter 4 states suggestions and future directions. Chapter 5 list out references and the appendix reproduces the data used.

[6] https://humanrightlawreview.in/wp-content/uploads/2026/02/Examining-the-Role-of-Digital-Forensics-in-Strengthening-Cybercrime-Investigations-in-India.pdf

CHAPTER II:MAIN BODY

2.1. Research Methodology

This paper follows us your doctrinal methodology no empirical research of any kind was undertaken there was no survey, questionnaire ,interview , sampling, field visit or station level observation and the paper makes no claim to primary empirical data. The Method confessed entirely of legal research conducted in the library help of statues and online sources proceeding in two stages both doctrinal character. First Letter analysis of primary legal sources the constitution, IT Act 2000, BNS, BNSS ,and BSA 2023 and judicial decisions were located read and analyse to identify the governing rules and how they interact, applying accepted canons of statutory interpretation including the rule that special laws prevail over a general one and requirement that penal provisions be strictly construed. Secondary sources: Namely peer reviewed articles and reputed legal commentary were used only to interpret and critic that primary material. Second doctrinal analysis of primary government legal documents: parliamentary replies of ministry of Home Affairs which are official records of the union executive placed on the record of parliament and the NCRB figures reproduced in them were read and tabulated in the same manner in which a doctrinal study reads a Gazette notification, a committee report or law report that is as text to be analysed rather than as a population to be sampled. Tabulating figures already published by the government and computing percentage from them is textual and documentary analysis not an empirical method because it generates no new data about any person or institution and involves no field work instrument or sample of the kind empirical legal research would require. Consequently the paper does not claim to have measured police, prosecutorial or judicial conduct, and every statement about from desk practice is expressly offered as a doctrinal inference from the legal position and the documentary record, not as an empirical finding. The corresponding limitation is accepted partially:a doctrinal method of this kind can state what the law provides and what the official records reports but it cannot fulfil without empirical field work which shows how a prevention operate inside a given police station establish that an association appearing in the published data is casual. Chapter IV accordingly identifies as a direction for separate future research the empirical field work that would be required to test the proposition advance here.

2.2 Findings

2.2.1. The existing Framework

Cybercrime enforcement in India rests on four instruments read together. The IT Act 2000 creates the core computer related offences including unauthorised access and damages(sec 44, 66) identity theft and cheating by personation using a computer resource (sec 66C, 66D) violation of

privacy (66E) cyber terrorism (66F) and obscene electronic record (sec 67-67B)[7]. Section 77B[8] makes offences carrying three years or mor cognisable and those carrying three years bailable.

The BNS 2023 supplies parallel and complementary offences: cheating and cheating by personation (sec 318-319)[9], stalking including electronic monitoring (sec 78) and organised crime which lists cyber crime among its predicate activities (sec 111)[10]. The BNSS 2023 governs procedure. It permits information about a cognisable offence to be given orally or by electronic communication to any police station irrespective of where the offence occurred (sec 173) and requires forensic experts to visits scenes and evidence collection to be video graphed for offences punishable with seven years or more with states allowed five years from July 1 2024 to notify the start date (sec 176(3)). The BSA[11] 2023 governs proof: electronic records are admissible on a certificate under section 63 continuing the rule in Anvar and Khotkar" that the certificate is a condition of admissibility for secondary electronic evidences[12] ". Commentary reports that the new certificate must also be signed by an expert[13]. Underlying these is a federal structure in which states police and prosecute crime". Subject to the principle that no one may be convicted except under a law in force at the time of the act.

2.2.2 Legal and procedural barriers(RQ2)

a. Rank based competence under section 78: The section begins with the non obstanta clause and prescribes who may investigate, not who may receive a complaint. Parliament raised threshold to inspector in 2008 replacing the earlier deputy Superintendent requirement, to make investigation more workable[14]. The section however links authority to seniority not to expertise. It does not require training, certification, or posting tour specialised unit. Two consequences follow. A trained in sub inspector in a cyber cell lawfully investigate an IT Act offence while an untrained inspector can. And where an inspector is scare or overloaded the statutory rule becomes a bottleneck. The Karnataka High Court has clarified that section 78 does not invalidate an fir registered by a sub inspector, it requires only that investigation be carried out by an inspector[15] the rule is therefore

[7] 0] Information Technology Act 2000 (as amended by the Information Technology (Amendment) Act 2008), ss 43, 65, 66–66F, 67–67B. Official text: India Code.
https://www.indiacode.nic.in

[8] https://lawrato.com/indian-kanoon/bare-act/information-technology-act/section-77b
[9] https://share.google/7HeoFcnZaof0DBZdP
[10] https://share.google/NUCHBrGmIOsD8HmEx
[11] https://www.indiacode.nic.in/handle/123456789/20062
[12] Bharatiya Sakshya Adhiniyam 2023, s 63; Anvar PV v PK Basheer (2014) 10 SCC 473; Arjun Panditrao Khotkar v Kailash Kushanrao Gorantyal (2020) 7 SCC 1.
https://indiankanoon.org/doc/172105947/

[13] Advocate Assist, 'Electronic Evidence Under BSA Section 63', (commentary; to be checked against the Schedule to the Adhiniyam).
https://advocateassist.ai/blog/bsa-section-63-electronic-evidence

[14] information Technology Act 2000, s 80 (Inspector rank following the 2008 amendment).
URL: https://lawgist.in/information-technology-act/80

[15] Neha Rafiq Chachadi v State of Karnataka Crl P No 102165 of 2019 (Karnataka HC, Dharwad Bench, 3 July 2023), 2023 LiveLaw (Kar) 268, paras 11–15.
URL: https://indiankanoon.org/doc/111654593/

a limit on, who investigate and it is practical cost lies in the shortage of officers who are both eligible and unskilled.

b. Refusal at the police station

A complaint who is told I have no authority to investigate is usually clearing a mis application of section 78. Under the BNSS the station must record information on a cognizable offense whatever the place of occurrence and a zero FIR must be transferred. The supreme court had already held registration to be mandatory in Lalitha kumari case[16] " section 78 affects who investigates afterwards not whether the complaint is recorded". The Lord does provide a remedy ladder for exactly this situation. In Sakiri Vasu v State of Uttar Pradesh [17]case " The the Supreme Court held that a complaint whose firs refused are whose investigation is inadequate need not rush to High Court the proper course is first to apply to Superintendent of police and if that fails to apply to the jurisdictional magistrate who has wide power to direct registration and to direct or monitor a proper investigation". The BNSS Now codifies this ladder in section 173(4) and 175(3) and the Supreme Court has recently clarified in Om Prakash Amebadkar v state of Maharashtra"[18] That that under the new provincial the magistrate must consider the police officers response before ordering investigation which adds a procedural safeguard but also a step and therefore time before reluctant station can be compelled to act. For a cyber fraud victim racing to freeze a mule account before funds are laid away this lawful but multistep remedy is of limited practical use, however doctrinally sound, the paper returns to this timing problem in section 2.4. 2 first Supreme Court they work as a gateways to delay at the first stage itself. Section173(3) allows a preliminary enquiry, the permission of deputy Superintendent for cognisable offences carrying under three to seven years. Which covers most IT Act offences[19]. And portal based reporting places the fir decision with state agency without a fixed timeline: the government states that conversion of portal complaints into FIR is handled by state and union territory agency as per law. The public consequences is that victim or redirected or discourage or delayed and stolen funds move beyond recovery within hours. The scale of such practice cannot be measured since no official data track it but the legal design permits it.

c. Forensic and evidentiary limitations

Digital evidence remains highly unstable and remain contingent on cooperation from tech intermediaries .Admissibility requires a certificate from the person controlling the device which can be difficult where data sits with a foreign platform and the certificate rule has been repeatedly been litigated. The mandatory forensic visits under section176(3) BNSS is phased in state by state

---

[16] *Lalita Kumari v. Government of Uttar Pradesh*, (2014) 2 SCC 1, available at: https://indiankanoon.org/doc/10239053/

[17] Sakiri Vasu v State of Uttar Pradesh (2008) 2 SCC 409, paras 14-20 (Supreme Court of India, 7 December 2007). https://indiankanoon.org/doc/1836621/

[18] Om Prakash Ambadkar v State of Maharashtra 2025 INSC 139 (Supreme Court of India) (Magistrate under s 175(3) BNSS must consider the police officers submissions, unlike under s 156(3) CrPC).
URL: https://www.verdictum.in/court-updates/supreme-court/section-175-3-bnss-magistrate-investigation-2025-insc-139-om-prakash-ambadkar-v-state-of-maharashtra-1566698

[19] BNSS 2023, s 173(3); see Mondaq, 'Bharatiya Nagarik Suraksha Sanhita, 2023 (BNSS)' (3 January 2024).
URL: https://www.mondaq.com/india/crime/1407526/bharatiya-nagarik-suraksha-sanhita-2023-bnss

and depends on laboratory capacity, so its benefit will be uneven. Section 79 intermediary safe harbour read down in Shreya Singhal case"[20] to require a court or government notice for take down has been supplemented by executive Sahyog portal but that portal accelerates notices, it does not make evidence admissible".

d. Undefined emerging offences

It is often said that new cyber crimes go un investigated because the statues do not name them. Many new modus operandi including digital arrest, slim based fraud and mule account laundering involved deception by personation and dishonest inducement, which existing cheating and personation provision already capture, as does section 66D of the IT Act. The real difficulties are different, first officers must map novel contact to correct the existing offense and there is no national mapping guide: the NCRB table itself shows 35,329 of 44,237 IT Act cases(79.9percent) in 2023 Under the single head computer related efforts only 36 deformation or morphing cases and 225 profile cases figures consistent with though not proof of under recording[21]. Second the choice of statue has consequences. In Digumarti[22] the Supreme court case held that "IT Act To be a special law and for obscene electronic content precluded parallel prosecution under the general penal provision so a wrong choice can defeat a prosecution". Third, section111 BNS uses Cyber crimes without defining them[23]. Fourth, penal statues cannot be stretched by analogy so genuine gaps(for example deep fake impersonation or the systematic supply of mule accounts) required legislative fixing rather than police improvisation. The definitional gap is therefore narrower than the public perception but real at the edges.

2.2.3.The institutional framework

The Union has built the coordinating layer around state policing. The Indian cyber crime coordination center 14(c) an attached office of the MHA runs the national cyber crime reporting portal the 1930 helpline the citizen financial cyber fraud reporting and management system launched in 2021, which the government says has saved more than ₹7130 crores across over 23,00,000 complaints, a cyber fraud mitigation center bringing banks, telecom providers and a state police together a suspect registry launched on 10th September 2024, the samanavaya data sharing platform, the sahyog portal for notices to intermediaries and the cytrain online course with 1,44,895,registered officers and 1,19,628,certificates issued. National cyber forensic laboratories operate at New Delhi and since August 20 25 in Assam. Cyber forensic cum training laboratories funded under the CCPWC scheme have been commissioned in 33 States and union territories[24]. CERT in and the NCIIPC address incident response and critical infrastructure under the IT Act.

---

[20] https://indiankanoon.org/doc/110813550/

[21] Ministry of Home Affairs (MHA), Lok Sabha Unstarred Question No 452 (answered 2 December 2025), Annexures I–II (NCRB, 'Crime in India' data). https://www.mha.gov.in/MHA1/Par2017/pdfs/par2025-pdfs/LS02122025/452.pdf

[22] Sharat Babu Digumarti v Government of NCT of Delhi (2017) 2 SCC 18. https://indiankanoon.org/doc/153597150/

[23] Esya Centre, 'The New Criminal Laws and Their Interface with Technology' (31 July 2024). https://www.esyacentre.org/perspectives/2024/7/31/the-new-criminal-laws-and-their-interface-with-technology

[24] MHA, Rajya Sabha Unstarred Question No 1346 (11 February 2026). https://www.mha.gov.in/MHA1/Par2017/pdfs/par2026-pdfs/RS11022026/1346.pdf

The Supreme Court has since pushed the framework towards greater center coordination. In its digital errors proceeding it asked the CBI to conduct pan India probe, required states that had withdrawn general consent to allow it and directed all States and union territory to set up state and regional cyber crime coordination centre's[25]. In February 2026 it asked the center to draft a standard operating procedure with the RBI, banks and telecom department and by August 2026 it had directed the RBI to frame a procedure on mule accounts[26]. The architecture thus Favors coordination, data and victim side fund recovery. Its weakness or structural. Most of these bodies exist by executive decision and not statue, the decision to register an fir and to investigate remains with state police, and training is offered to a voluntary online platform whose enrolment figures do not show how many trained officers or inspectors actually deployed on cyber cases[27].

2.2,4 Regional disparities

State wise data reveal 4 patterns. Concentration Karnataka 21889, Telangana 18236 Uttar Pradesh 10794 and Maharashtra 8103 together account for 59022 of 86420 cases in 2023 or 68.3% while Nagaland registered 2 Manipur and Sikkim 12 figure one[28]. Near zero registration cannot sensibly be read as low incidence volatility: Assam fell from 4846 cases in 2021 to 909 in 2023 whereas Kerala rose from 773 in 2022 to 3295 in 2023 and Bihar from 1621 to 4450 movements more plausibly explained by recording and reporting practice than by offending alone. Classification: Karnataka shows no cases under the fraud head in 2023 despite 21889 total cases, which suggests that fraud is recorded under other heads making Interstate comparison unreliable

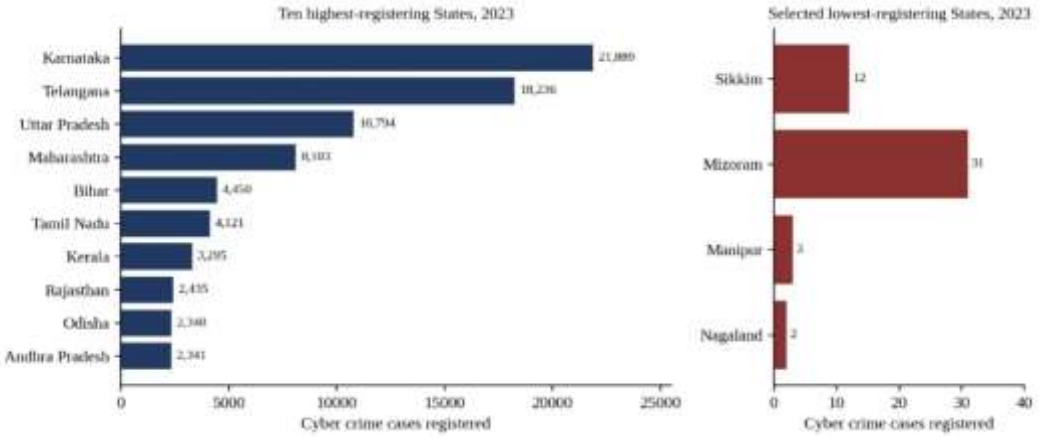
Figure1:cyber crime cases registered, selected states, 2023

[25] Digital Arrest Scam: SC Orders Pan-India CBI Probe, Issues Sweeping Directions to States, Agencies' (The Tribune).
https://www.tribuneindia.com/news/india/digital-arrest-scam-sc-orders-pan-india-cbi-probe-issues-sweeping-directions-to-states-agencies

[26] Open Magazine, 'Supreme Court Cracks Down on Digital Arrest Scams' (4 August 2026).
https://openthemagazine.com/india/supreme-court-cracks-down-on-digital-arrest-scams-heres-what-the-new-direc

[27] SC to Hear Next Week Suo Motu Case Concerning Victims of Digital Arrest' (Business Standard, 16 March 2026).
URL: https://www.business-standard.com/india-news/sc-to-hear-next-week-suo-motu-case-concerning-victims-of-digital-arrest-126031600385_1.html

[28] Ministry of Home Affairs (MHA), Lok Sabha Unstarred Question No 452 (answered 2 December 2025), Annexures I–II (NCRB, 'Crime in India' data).
https://www.mha.gov.in/MHA1/Par2017/pdfs/par2025-pdfs/LS02122025/452.pdf



4001 of 19466 fraud cases were charge sheeted in 2023 484 trials were only Completed and 22 ended in conviction, a conviction rate of 4.5% among completed trials. Charge sheeting ranged from 1.6% in Tamil Nadu and 5.5% in Odisha to 59.0% in Bihar. Telangana completed 410 trials in 2023 but recorded six conviction.

Table1: charge sheeting in cyber fraud cases, selected states 2023

STATE/UT	Total cyber cases 2023	Fraud cases registered	Charge sheeted	Charge sheeting rate
Telangana	18,236	10,626	1,760	16.6
Maharashtra	8,103	2,075	276	13.3
Bihar	4,450	2,611	1,540	59.0
Uttar Pradesh	10,794	287	86	30.0
Tamil Nadu	4,121	887	14	1.6
Odisha	2,348	1,362	75	5.5
Karnataka	21,889	0	0	n/a
All	86,420	19,466	4,001	20.6

Infrastructure: Forensic capacity is unevenly distributed. One laboratory at deragaon, Assam serve all eight north eastern states[29] and as of March 20 25 the government reported that no CCPWC forensic cum training laboratory had been established in Tamil Nadu a state whose recorded cases doubled in 2023[30] these observation show bar capacity is thin.

[29] MHA, Rajya Sabha Unstarred Question No 1346 (11 February 2026). https://www.mha.gov.in/MHA1/Par2017/pdfs/par2026-pdfs/RS11022026/1346.pdf

[30] MHA, 'Cyber Crime Prevention against Women and Children (CCPWC) Scheme' (Lok Sabha reply, 11 March 2025), PIB. https://www.pib.gov.in/PressReleseDetailm.aspx?PRID=2110359&reg=48&lang=2

2.2.5. Jurisdictional fragmentation as a barrier distinct from capacity(RQ2/RQ4)

A further barrier, less visible in aggregate statistics, is that cyber fraud offending is rarely confined to one state, while the procedural code still organises investigation around territorial jurisdiction. Section 202 of the BNSS, carrying forward section 182 of the former Crpc, allows an offence committed by electronic communication to be tried where the message was sent or where it was received, and section 200 BNSS (formerly section 180Crpc). Gives jurisdiction wherever a consequence of the offence ensues[31]. In a typical digital arrest or investment fraud chain, the call may orginate from one state or abroad, the victim may loses money in a second state, and the mule account receiving the funds may sit in a third. Each linked state can lawfully claim or decline the case, coordination between them depends on ad hoc liaison rather than a single statutory forum.

The supreme court had recently confirmed how the little the ordinary law does to relieve this fragmentation. In Rutviji Bhagat wakhare v State of Maharashtra [32], decided on 24th July 2026. The petitioner faced four cyber fraud FIR in Maharashtra Karnataka and Odisha all involving digital arrests modus operandi And funds creditors to one account and sort either washing or clubbing into a single composite investigation. The court refused both. It felt that a similar modus operandi across the complaints did not by itself show that the offences form part of the same transaction within the meaning of the law on multiple firs since each FIR was lodged by a different complaint induced to be part with money on a different occasion, with no show link between the transaction: it added that clubbing could itself prejudice complaints by forcing them to litigate outside their home state. A few months earlier in Odela Satyam v State of Telangana case [33]"The court had already confined clubbing of multi victim financial fraud FIRS to within a single state declining to permit a pan India consolidation noting section 242 of the BNSS allows joinder of up to 5 similar offences committed within 12 months only for the purpose of a single trial not as a mechanism for cross state investigation. Read together the two ruling confirmed that the ordinary law treat each state FIR as a Self contained proceedings unless the transaction is identical. Which is rarely demonstratable are the investigation stage in a layer mule account chain. The practical result is that no single investigator is answerable for the fraud as a whole: each state pursues its own slice and the national conviction rate recorded in section 2.4 is the sum of many such partial, uncoordinated efforts rather than evidence that any one of them fail on its own terms. This is why Supreme Court digital Rs proceeding have needed to direct central investigating agency and state concern to it rather than leaving coordination to the ordinary jurisdictional rules[34]. Jurisdictional

[31] BNSS 2023, s 202 (offences committed by means of electronic communications: jurisdiction where the communication was sent or received), corresponding to s 182 CrPC 1973.
https://www.writinglaw.com/section-202-bnss/

[32] Rutvij Bhagat Singh Wakhare v State of Maharashtra, Writ Petition (Crl) No 127 of 2026, 2026 INSC 740 (Supreme Court of India, 24 July 2026, Karol and Masih JJ), paras 13-16.
https://www.advocatekhoj.com/library/judgments/2026/july/75.php

[33] Odela Satyam v State of Telangana 2025 INSC 1174 (Supreme Court of India) (clubbing of multi-State financial-fraud FIRs confined to within a State; BNSS 2023, s 242, on joinder of similar offences for trial).
https://blog.primelegal.in/one-crime-one-fir-one-jurisdiction-landmark-ruling-in-odela-satyam-case/

[34] 'Digital Arrest Scam: SC Orders Pan-India CBI Probe, Issues Sweeping Directions to States, Agencies' (The Tribune).
https://www.tribuneindia.com/news/india/digital-arrest-scam-sc-orders-pan-india-cbi-probe-issues-sweeping-directions-to-states-agencies

fragmentation is therefore a barrier of a different kind from once discussed above: it is not about who may investigate or how skilled they are but about which of several lawful competitors station will actually do so and the case law shows that courts, applying the law as it stand will usual decline to resolve question for them.

2.3.Discussion(RQ5)

The findings support a qualified answer: the framework addresses cyber crime enforcement only to a limited extent, and its weakest paths are procedural and institutional rather than substantiative. On substantiative coverage, the combination of the IT act and BNS is broader then commonly assume, Under supreme court's digital arrest proceedings concern enforcement failure more than a lack of offenses where genuine gap exist, they are at the margin and call for targeted amendment.

On the hypothesis,H0 cannot be sustained. Outcomes vary widely across states, the rank based rule servers authority from skill and forensic capacity is un even but H1 is supported only in part. The available data do not include state wise counts of cyber train inspectors, so the link between capacity and outcomes is plausible not demonstrator. Bihar's 59.0 per cent charge heating rate, for instance, shows that why conversion is possible in a state not usually associated with strong technical capacity, which suggests that classification, case mix or recording practice may matter as much as infrastructure. This is a finding in itself: the absence of capacity data is a barrier to reform

the victims perspective sharpens the point. A compliant who is turned away because the officer lacks authority is not being subjected to a legal requirement so much as to a gap between the letter of section 78 and how stations are organised. The law already gives a victim the right to be heard at any station and sakkiri vasu case and section 173(4) and 175(3) BNSS, A route to compel action what it does not give us a route that is fast enough to matter before stolen funds are launder to a chain of new accounts. That timing gap more than any missing definition, explains while rising reporting has not produced proportionate prosecution.

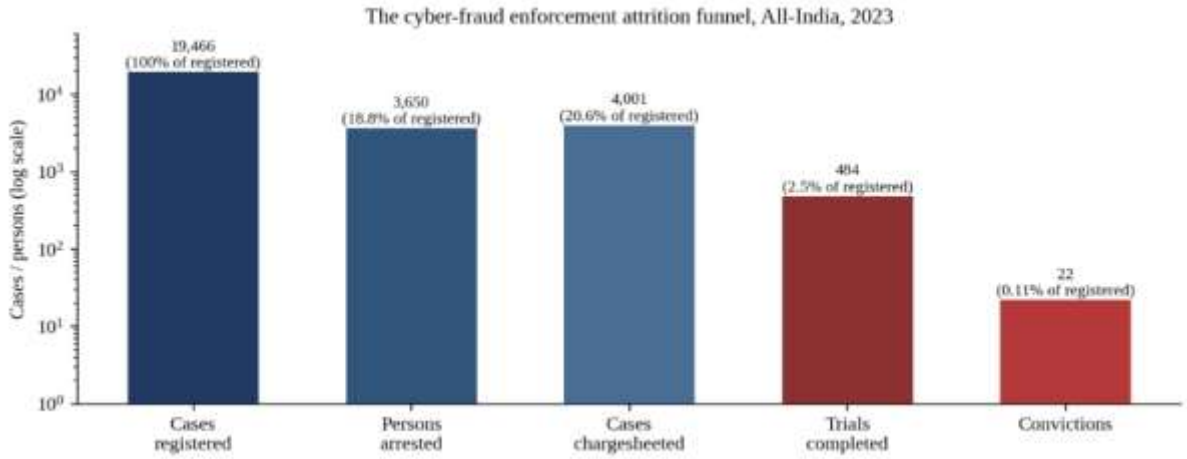
2,4. Original analytical contribution

The discussion above establishes that outcomes are weak and uneven, but it has so far treated the weakness as a single fact(a low charge sheeting rate) and the unevenness as a list of examples. This section builds to original analytical tools from the same official data set to make both points precise and to show Exactly bad along the journey from complaint to conviction and in which kind of state, the framework fails most. Neither construction below has been located in the cyber law literature reviewed for this paper: both are the authors own arrangement of figures published by the ministry of Home affairs.

2.4.1.The enforcement attrition funnel

Reading the fraud head figures in annexure III of parliamentary reply as a single sequence, rather than as separate totals, deals an attrition funnel of 19466 cyber fraud cases register across India in 2023, 3650 persons were arrested(18.8 percent of registered cases), 4001 cases were charge sheeted(20.6 percent), 484 trials were completed (2.5 percent of registered cases or 12.1 per cent of charge sheeted cases) and 22 convictions resulted (4.5 per cent of completed trials, but only 0.11 per cent cases first registered). Figure 2 plots this funnel on logarithmic scale, since the stages differ by three orders of magnitude and a linear chart would flatten the trial and conviction stages to invisibility.

Figure 2: The cyber fraud enforcement attrition funnel, all India, 2023



The value of the funnel is that it separates two different failures that the single charge sheeting statistics(20.6 per cent) conceals. The first drop, from registration to chargesheet, is the one most directly affected by the rank based competence problem examined in section2.2.2: it is the stage at which an eligible inspector must actually investigate and complete a case file. The second, much larger drop, from chargesheet(4001) to completed trial (484) to conviction(22) lies almost entirely outside the police station, in prosecutorial capacity, the section 63BSA certificate requirement discussed in section 2.2.2(c) and court backlog. A reform agenda built only on the first stage, such as a section 78 amendment, would leave second and large leak in the funnel untouched. This decomposition is not visible in NCRB reporting itself, which lists the four figures separately rather than as a sequence and it does not appear to have been constructed this way in the secondary literature reviewed for this paper.

2.4.2A Capacity outcome typology of states

The second construction classifies the 7 states in table one along 2 axis drawn from the same data : case volume(the number of cyber fraud cases registered a proxy for the demand placed on the system) and charge sheeting rate (the share of registered cases converted into a charge sheet, a proxy for how the system meets that demand). Using the national average of 20.6% as the dividing line for the conversion and 5000 cases as a rough dividing line for volume, 4 types emerge, together with a fifth, anomalous category that that typology itself brings into view.

Table 2: A capacity outcome typology of states, constructed from 2023 fraud head data.

Type	States(2023 data)	Reading
High volume at or above average conversion	Uttar Pradesh (10,974 cases. 30.0 percent)	System that appear to scale Reasonably well, What studying as a comparator of reform
High volume below average conversion	Telangana(18,236, 16.6 percent) Maharashtra (8,103, 13.3 percent)	overloaded systems: heavy case low

		outpacing investigative or forensic input
low volume, above average conversion	Bihar (4,450; 59.0 percent)	Encouraging, but small base can inflate a rate needs verification against absolute charge sheet counts before being read as best practice
Low volume, below average conversion	Tamil Nadu (4,121;1.6 per cent) Odisha(2,348. 5.5 percent)	vehicles performing group in relative terms ,though absolute caseload is manageable, suggesting the constraint is procedural rather than purely a matter of volume
Data anomalous	Karnataka (21,889 total cases)	highest registering state in India cannot be placed on the typology at all, because its own returns record zero fraud cases despite fraud being the leading national motive, this is itself the clearest single piece of evidence in the data set the classification practice not just capacity drive the headline disparity figures.

The typology answers RQ 4 more precisely than a list of high and low state can. It shows that regional disparity in cyber crime enforcement is not one phenomenon but at least 3: genuine overload in high demand states, a possible small base effect that inflates apparent success in a low demand state, and the data classification failure in the highest volume state of all, which no

capacity building measure can fix because it is a recording practice, not a resourcing gap. Policy gained at regional disparity as a single problem would misdiagnose at least two of these three types which is precisely why the suggestion in chapter 4 are differentiated by cause(competence. Timeline, capacity, data) rather than offered as a single uniform remedy.

CHAPTER III:CONCLUSION

This paper set out to determine how well India's legal and institutional framework enables effective and equitable cyber crime enforcement. It found that the substance of law is broader than often assumed but that the procedural and institutional design has three principle weakness. First section 78 of IT act ties investigative authority to rank, not competence, which produces a bottleneck of eligible but untrained officers and, in practice, encourages the mistaken belief that a station cannot deal with cyber complaints. Secondly,there is no mandatory death line for converting portal complaint into an FIR or initiating an investigation, allowing state level practice to dictate the pace.

Third, forensic and prosecutorial capacity, and even recording practice, differ so markedly across states that the same offense meets very different outcomes depending on where it is reported.

The study met its aims in mapping the framework, identifying barriers and describing disparities, but it could not test causation, because no capacity data are published. The significance of the finding is that reforms should be aimed less at creating new offences and more at competence, accountability, classification and data.

CHAPTER IV:SUGGESTIONS AND FUTURE DIRECTIONS

4.1.SUGGESTIONS

1. Main section 78 competence based: amend the section so that investigation may be carried out by an inspector or by n officer of lower rank who is authorised by the state government and holds a prescribed cyber investigation certification, a model already familiar from other special statues. States should issue standing orders designating at least one certified inspector per district aur subdivision to receive alit Act cases.
2. Close the front desk gap: MHA and State police headquarters should issue a binding advisory that no station may decline to register a cyber complaint on the ground of rank or jurisdiction: that registration under section 173BNSS, including zero fir is immediate, and that a designated officer takes over within a stated period. Use of preliminary enquiry group for cyber fraud should be limited and time bound, and refusal should be reviewed at Superintendent level.
3. Set a statutory timeline for portal to FIR conversion: rules or a statutory amendment should require state agency to decide on far registration for complaints on the national portal within a fixed. With periodic public reporting.
4. Adopt national offense mapping protocol: NCRB and 14C should issue an update a guide linking each emerging modus operandi(digital arrest, Mule accounts, loan app extortion, deep fake impersonation) to the correct provision of the IT act and BNS and should define cyber crimes for section111 BNS. Only conduct that truly fails outside the existing prevention should be addressed by the targeted amendment consistent with article20(1).
5. Equalise capacity: prioritise forensic assets for states with no scheme funded laboratory and for region served by single facility: make certified training a condition of posting to cyber units instead of voluntary option and create specialist cyber prosecutors saw that charge sheeted cases are not lost at trial.
6. Published capacity and outcome data: NCRB and and states should publish the number of certified investigators, laboratory turnaround times, the ratio of portal complaints to FIRs, charge sheeting and conviction rates on uniform state wise basis.
7. Giving the coordination layer a legal footing. Provide statutory a rule based backing for 14C functions. And formalise consent and coordination arrangement between the CBI and states for pan India cyber cases, Building on the supreme courts directions. As Wakhere and Odela Satyam confirm the ordinary law of multiple firs will not by itself a consolidate across the new account chain into one investigation; a statutory single window mechanism for linked cyber fraud firs, triggered on a documented fund trail rather than left to writ proceedings, is needed to close this gap.

4.2.Future Directions

Three Lines of research follow, first empirical fieldwork, including station level audit, right to information request and interviews with victims and investigators, is needed to measure front desk refusal and to test H1 with capacity data, second, comparative work could examine how other federal system allocate competence for cyber investigations. Third,

technology is already altering board of funding and enforcement. The Supreme Court has questioned why artificial intelligence is not used to detect and freeze mule account[35], and ai assisted complaint triage, pattern detection and deep fake forensics may improve response. The search should examine how far such tools can be used with adequate safeguards for accuracy, accountability and privacy, since automated freezing of accounts affects innocent account holders.

CHAPTER V:REFERENCES

A. Constitutional and statutory materials

Constitution of India, art 20(1),art 246 and seventh schedule, list II, entry2,

Information Technology Act,2000

Bharatiya Nyaya Sanhita 2023

Bharatiya Nagarik Suraksha Sanhita 2023

Bharatiya Sakshya Adiniyam 2023

B.Cases

Anvar PV v PK Basheer

Arjun Panditrao Khotkar v Kailash Kushanrao Gorantyal

Lalithakumari v Government of Uttar Pradesh

Neha Rafiq chachadi v State of Karnataka

Odela shyam v state of Telangana

Om Prakash Ambadkar v state of Telangana

Rutviji Bhagat singh Wakhare v state of Maharashtra

[35] Digital Arrest Scam: SC Orders Pan-India CBI Probe, Issues Sweeping Directions to States, Agencies' (The Tribune).
https://www.tribuneindia.com/news/india/digital-arrest-scam-sc-orders-pan-india-cbi-probe-issues-sweeping-directions-to-states-agencies

Sakkiri vasu v state of Uttar Pradesh

Sharat Babu Digumarti v Government of NCT of Delhi

Shreya Singhal v UOI

c. Government documents

Digital Arrest Scam: SC Orders Pan-India CBI Probe, Issues Sweeping Directions to States, Agencies' (The Tribune).

https://www.tribuneindia.com/news/india/digital-arrest-scam-sc-orders-pan-india-cbi-probe-issues-sweeping-directions-to-states-agencies

MHA, Rajya Sabha Unstarred Question No 1346 (11 February 2026).

https://www.mha.gov.in/MHA1/Par2017/pdfs/par2026-pdfs/RS11022026/1346.pdf

Ministry of Home Affairs (MHA), Lok Sabha Unstarred Question No 452 (answered 2 December 2025), Annexures I–II (NCRB, 'Crime in India' data).

https://www.mha.gov.in/MHA1/Par2017/pdfs/par2025-pdfs/LS02122025/452.pdf

MHA, Rajya Sabha Unstarred Question No 1346 (11 February 2026).

https://www.mha.gov.in/MHA1/Par2017/pdfs/par2026-pdfs/RS11022026/1346.pdf

Ministry of Home Affairs (MHA), Lok Sabha Unstarred Question No 452 (answered 2 December 2025), Annexures I–II (NCRB, 'Crime in India' data).

https://www.mha.gov.in/MHA1/Par2017/pdfs/par2025-pdfs/LS02122025/452.pdf

Ministry of Home Affairs (MHA), Lok Sabha Unstarred Question No 452 (answered 2 December 2025), Annexures I–II (NCRB, 'Crime in India' data).

https://www.mha.gov.in/MHA1/Par2017/pdfs/par2025-pdfs/LS02122025/452.pdf

D. Peer reviewed and scholarly sources

Nir Kshetri, 'Cybercrime and Cybersecurity in India: Causes, Consequences and Implications for the Future' (2016) 66 Crime, Law and Social Change 313.

https://doi.org/10.1007/s10611-016-9629-3

Sesha Kethineni, 'Cybercrime in India: Laws, Regulations, and Enforcement Mechanisms' in Thomas J Holt and Adam M Bossler (eds), The Palgrave Handbook of International Cybercrime and Cyberevidence (Palgrave Macmillan 2020).

https://link.springer.com/referenceworkentry/10.1007/978-3-319-90307-1_7-1

Elavarasi and Elango, 'Analysis of Cybercrime Investigation Mechanism in India' (2020) Indian Journal of Science and Technology.

https://indjst.org/articles/analysis-of-cybercrime-investigation-mechanism-in-india

A Banu R and J Banerjee, 'Examining the Role of Digital Forensics in Strengthening Cybercrime Investigations in India' (2025) 4(1) International Journal of Human Rights Law Review 60.

https://humanrightlawreview.in/wp-content/uploads/2026/02/Examining-the-Role-of-Digital-Forensics-in-Strengthening-Cybercrime-Investigations-in-India.pdf

E. Commentary and News sources

Esya Centre, 'The New Criminal Laws and Their Interface with Technology' (31 July 2024).

https://www.esyacentre.org/perspectives/2024/7/31/the-new-criminal-laws-and-their-interface-with-technology

'Digital Arrest Scam: SC Orders Pan-India CBI Probe, Issues Sweeping Directions to States, Agencies' (The Tribune).

https://www.tribuneindia.com/news/india/digital-arrest-scam-sc-orders-pan-india-cbi-probe-issues-sweeping-directions-to-states-agencies

Advocate Assist, 'Electronic Evidence Under BSA Section 63',.

https://advocateassist.ai/blog/bsa-section-63-electronic-evidence

MHA, 'Cyber Crime Prevention against Women and Children (CCPWC) Scheme' (Lok Sabha reply, 11 March 2025), PIB.

https://www.pib.gov.in/PressReleseDetailm.aspx?PRID=2110359&reg=48&lang=2

APPENDIX

HEAD	2019	2020	2021	2022	2023
Offenses under IT Act	30,846	29,643	27,427	31,908	44,237

Computer related offenses	23734	21,926	19,915	23,894	35,329
Offenses under IPC	13,800	20,201	25,384	33,798	41,849
Fraud	6,229	10,395	14,007	17,470	19,466
Cheating	3,367	4,480	6,343	10,509	16,943
Miscellaneous	89	191	163	187	334
Total	44,735	50,035	52,974	65,893	86,420