# Analysis of Cybercrime Laws and Rising Digital Fraud in India

**Sai Aditya, Pooja Jain, Jagriti Banerjee, Aman Raj, Vanshika Agarwal, Mohammad Mujtaba Tanveer**

**Abstract** Cybercrime and digital fraud challenge India's expanding digital environment. This study combines doctrinal review of Indian cybercrime law and institutions with descriptive analysis of official secondary data: NCRB-registered cases (2014–2024), NCRP financial-fraud complaints (2021–2025), NCRP reports of digital-arrest scams and related cybercrimes (2022–2024), selected 2024 State totals, and NPCI-derived UPI activity (FY2021–22 to FY2025–26). These series are kept separate because they measure registered cases, complaints, a combined scam-report category and payment activity. NCRB cases rose from 9,622 to 101,928; NCRP financial-fraud complaints rose from 262,846 to 2,402,579. Unverifiable fraud-enablement percentages were excluded and the methods are discussed qualitatively. The study proposes a typology–provision–capacity mapping linking fraud conduct to potentially relevant laws, evidence and institutional responsibilities. Aggregate data cannot establish causation or directly measure legal effectiveness; that requires linked case-progression and recovery outcomes.

**Keywords:** cybercrime; digital fraud; India; Information Technology Act; cybercrime law; digital forensics; digital arrest scams; financial fraud

## 1. Introduction

India's expanding use of online banking, digital payments and internet-based services has been accompanied by a marked rise in cybercrime recorded by official systems. NCRB-registered cybercrime cases increased from 9,622 in 2014 to 101,928 in 2024, while financial-fraud complaints submitted through NCRP rose from 262,846 in 2021 to 2,402,579 in 2025 [5], [7], [22]. These figures establish growth in recorded cases and complaints, not a direct measure of every offence committed: reporting awareness, access to reporting channels and police registration practices can also affect the totals. Reported methods include phishing, vishing, account takeover and digital-arrest scams, which often rely on impersonation and social engineering.

India's response is distributed across instruments with different purposes. The Information Technology Act, 2000 contains cyber-related offences, including identity theft and cheating by personation using a computer resource; the Bharatiya Nyaya Sanhita (BNS), including Sections

318 and 319 where their respective elements are met, may also apply to cheating or cheating by personation; and the Bharatiya Sakshya Adhiniyam (BSA), 2023 governs evidentiary requirements for electronic records. CERT-In Directions impose specified incident-reporting and log-retention obligations on entities within their scope, while the Digital Personal Data Protection (DPDP) framework concerns covered personal-data processing and has phased commencement. Institutionally, NCRP is a public reporting channel, CFCFRMS supports rapid reporting and coordination to help prevent funds from being siphoned away, and I4C provides national coordination and technical support. These roles are complementary but not interchangeable [1]–[4], [7], [18], [19], [22], [23].

The central question is whether complaints can be investigated across jurisdictions, supported by reliable digital evidence and pursued through prosecution [11], [12]. This study therefore combines doctrinal review with descriptive analysis of public secondary data from NCRB, NCRP/I4C, RBI and NPCI [5]–[9], [22]. Its organising contribution is a typology–provision–capacity mapping: for selected fraud methods, it identifies potentially relevant legal elements, evidence requirements and institutional hand-offs. Available aggregate indicators are not linked to individual complaint cohorts and cannot establish case progression or final refunds; the study therefore identifies evaluation gaps rather than claiming to measure overall legal effectiveness.

**Research Objectives and Questions**

The study has four objectives:

1. To examine trends in reported cybercrime and digital fraud in India using available secondary data.
2. To review the principal legal and regulatory instruments relevant to cybercrime and digital evidence.
3. To examine selected fraud typologies and the institutions involved in reporting, investigation and response.
4. To identify implementation and evaluation gaps between the existence of legal provisions and measurable enforcement outcomes.

The study is guided by the following research question: *What do publicly available reporting data and the legal–institutional framework reveal about India's capacity and constraints in responding to evolving cybercrime and digital fraud?*

## 2. Literature Review

### Overview

The review is a narrative (non-systematic) review covering five themes: India's legal and institutional framework; reported cybercrime and financial-fraud trends; investigation and prosecution capacity; evolving fraud typologies and regulatory coordination; and attack vectors and digital forensics. Together, these themes connect legal provisions with reported patterns and the practical capacity to investigate offences.

The literature reviewed falls into three related strands. The first is doctrinal: Biswas examines data theft, e-commerce and jurisdictional questions under India's earlier legal framework [27], while Rani surveys Indian cybercrime law and prosecution challenges [11]. More recent analysis by Narena and Gupta considers how the IT Act framework responds to AI-enabled fraud, deepfakes and cross-border threats, and argues that implementation and regulatory coordination remain important concerns [26]. Read together, these works show a shift from foundational questions about electronic data and jurisdiction toward contemporary challenges involving synthetic content and transnational offending. The legal setting has also changed since the earlier studies, particularly with the BNS, BSA and DPDP framework; conclusions based on the pre-2024 framework therefore require careful updating [2]–[4], [23], [25].

The second strand concerns reported patterns and fraud mechanisms. Tripathy provides a broad survey of cybercrime categories and Indian trends [6], while Panwar and Shekhar discuss digital-arrest scams as coercive, impersonation-based offences [10]. These works are useful for identifying typologies, but they do not replace official administrative data for national counts. For that purpose, this paper relies on NCRB, MHA and I4C records, and distinguishes NCRB police-registered cases from NCRP complaints and the parliamentary series on digital-arrest scams and related cybercrimes [5], [7], [13], [22]. I4C's advisory describes the impersonation, intimidation and video-call coercion used in such scams and states that there is no legal process of 'digital arrest' in India [28].

The third strand addresses enforcement, evidence and institutional capacity. Rani and Dandotiya and Veer discuss weaknesses in legal response, investigation and enforcement [11], [12], while the official framework places primary investigation and prosecution responsibility on State/UT law-enforcement agencies, supported by national coordination and technical capacity [7], [22]. The selected literature is heterogeneous in date, scope and publication outlet; it is used for thematic context, not as a source of national prevalence estimates. The organising contribution of this study is a transparent typology–provision–capacity mapping that links selected fraud conduct to potentially relevant legal elements, evidence requirements, responsible institutions and measurable response outcomes. The review is narrative rather than systematic and is not exhaustive.

## Theme 1: The Framework

The IT Act, 2000 provides cyber-specific offences: Section 66C addresses identity theft, Section 66D cheating by personation using a computer resource, and Sections 43 and 66 may apply to unauthorised access or damage when their elements are met [1], [2]. No single provision covers every online fraud.

The BNS, in force from 1 July 2024, may apply to cheating (Section 318) or cheating by personation (Section 319) where the elements are met; it does not replace cyber-specific IT Act offences. The BSA, also in force from that date, governs electronic records; Section 63 and its Schedule address admissibility and certification [2], [23]. CERT-In's 2022 Directions require six-hour reporting for specified covered incidents and 180-day log retention in India, subject to their scope [18], [19]. These instruments address different legal and operational functions.

The DPDP Act and Rules have staggered commencement. Under the 13 November 2025 notification, specified provisions commenced immediately, Sections 6(9) and 27(1)(d) after one year, and most substantive Act provisions after eighteen months (13 May 2027). Rules 1, 2 and 17–21 commenced on publication, Rule 4 after one year, and Rules 3, 5–16, 22 and 23 after eighteen months [3], [4], [25]. The DPDP framework governs covered personal-data processing; it is not a stand-alone cybercrime statute.

**Table 1:** Evolution of Key Cybercrime-Related Legislation and Institutional Mandates in India

| Year | Instrument | Key relevance |
|---|---|---|
| 2000 | IT Act, 2000 | Legal recognition of electronic records; defines core cyber offences |
| 2008 | IT (Amendment) Act | Adds cyber terrorism and data-related offences; provides for CERT-In under Section 70B |
| 2022 | CERT-In Directions | Six-hour reporting for specified covered incidents; 180-day log retention |
| 2023 | BNS & BSA | Updated criminal-law and electronic-evidence framework |
| 2023 | DPDP Act | Data-protection framework enacted |
| 2025 | DPDP Act / Rules | Staggered commencement; most substantive provisions scheduled for 13 May 2027 |

## Theme 2: Trends in Cybercrime & Digital Fraud

NCRB records police-registered cases, NCRP/CFCFRMS records citizen-reported financial-fraud complaints, and NPCI reports payment activity. Their definitions and reporting processes differ, so the series are analysed separately and not combined into a single cybercrime total [5]–[8], [22].

### Theme 3: Enforcement, Prosecution, & the Conviction Gap

Annual registrations cannot be compared directly with annual convictions: cases decided in a year may have been registered earlier, and pending cases affect any rate. The available sources do not provide a consistent cohort and denominator for a reliable national conviction rate. A valid assessment would track cases registered, charge-sheeted, tried, convicted, acquitted and pending over matched periods. State/UT agencies primarily investigate and prosecute, while MHA and I4C provide coordination and capacity support [7], [10]–[12], [22].

### Theme 4: Fraud Typologies & Regulatory Lag

Fraud methods increasingly combine phishing, credential theft or payment-request manipulation with impersonation and social engineering. In digital-arrest scams, offenders impersonate authorities, use calls or video to create pressure, and demand money under the pretext of bail or investigation. The parliamentary series records 39,925 incidents of digital-arrest scams and related cybercrimes reported on NCRP in 2022 and 123,672 in 2024 [13]. The source also reports 60,676 incidents for 2023; a partial-year 2025 figure is excluded from comparison. These are portal-reported incidents for a combined category, not a separately maintained NCRB count of digital-arrest offences.

A single complaint may involve telecom call records, bank and beneficiary details, platform identifiers and victim-device artefacts. Timely preservation, transaction tracing and coordination among the complainant, bank and police can therefore affect investigation and fund restraint. Reported amounts, lien-marked funds, amounts described as saved and money actually returned are distinct measures [7].

### Theme 5: Attack Vectors & Digital-Forensic Capacity

Digital fraud commonly combines social engineering with technical methods such as SIM swapping, phishing, smishing and synthetic voice or video. These methods seek information, account control or trust that can be used to access accounts or induce fraudulent transactions.

Each attack vector generates different evidence. SIM-swap inquiries may require subscriber-change records, SIM replacement logs and authentication events; phishing inquiries may require original messages, URLs, headers and provider logs; suspected deepfake impersonation requires preservation of original media, metadata and account provenance. Because such evidence may be held by different organisations or overwritten, timely preservation and documented chain of custody are important. International guidance explains the mechanisms [14]–[17], while Indian reporting documents blocking of spoofed calls and accounts used in digital-arrest scams [24]. The earlier fraud-enablement percentages are excluded because their sample, denominator and period could not be verified; these methods are discussed qualitatively, not ranked nationally.

**Digital Forensic Capacity.** Digital forensics connects technical investigation with evidentiary requirements. Investigators must collect and preserve digital evidence, analyse devices and records, establish relevant timelines and document provenance so that evidence can be assessed in court. Forensic capacity therefore affects whether a complaint can be developed into usable evidence.

MHA reports national and State-level forensic capacity, including the National Cyber Forensic Laboratory (Evidence) in Hyderabad and the National-Digital Investigation Support Centre in New Delhi. By June 2026, the latter had assisted in more than 14,064 cases; CyTrain had registered over 1,63,344 police/judicial officers and issued over 1,61,957 certificates. MHA also reported cyber-forensic training laboratories in 33 States/UTs and seven Central and 28 State Forensic Science Laboratories [22]. These are activity indicators, not proof of equal access or improved court outcomes.

Early technical assistance and specialised laboratories can support evidence preservation and analysis. Evidence must still be lawfully collected, authenticated and documented. Comparable State/UT data on access, caseload, turnaround time and court outcomes are unavailable; forensic capacity therefore cannot be linked directly to convictions [7], [22].

I4C's Samanvaya platform supports data sharing and interstate link analysis; Pratibimb maps suspected criminals and crime infrastructure [22]. These tools matter where victims, accounts or suspects cross jurisdictions. The BSA Section 63 and Schedule set certificate requirements for electronic records, linking collection and preservation to later court presentation [23].

## 3. Research Methodology

### A. Research Design

This study uses a combined doctrinal and descriptive secondary-data design, not primary empirical research. First, it reviews the text of relevant legislation, rules and official institutional descriptions. Second, it purposively selects official series that provide at least one of the following: annual registered cybercrime cases, financial-fraud complaints and reported amounts, NCRP-reported digital-arrest scams and related cybercrimes, State case totals, payment-system activity, or documented institutional capacity. The study periods are NCRB cases 2014–2024; NCRP/CFCFRMS financial-fraud complaints 2021–2025 (the MHA table notes that the data are dynamic); NCRP reports of digital-arrest scams and related cybercrimes for 2022–2024; and UPI transaction volume and value for FY2021–22 to FY2025–26. The parliamentary answer also provides a 2025 figure only through 28 February; that partial-year value is excluded from year-to-year comparison. Unverifiable fraud-enablement percentages from an earlier draft are excluded from quantitative analysis.

The source review is current to 6 November 2026. Each typology is mapped to potentially

relevant statutory elements, evidence requirements and institutional hand-offs without presuming liability. Enforcement is assessed through published indicators where available; missing data are recorded as gaps. Series are not pooled and the design cannot establish causation.

### B. Nature of the Research

The doctrinal component examines the IT Act, BNS, BSA, DPDP Act and Rules, and CERT-In Directions. The descriptive component uses official statistics and selected publications, not interviews, surveys or case files. Legal findings are compared with published indicators, not treated as proof of causation.

### C. Sample and Its Technique

No individual respondents were sampled. Sources were selected purposively for relevance, official provenance, defined period and useful variables. NCRB supplies registered cases; NCRP/CFCFRMS, financial-fraud complaints and amounts; the parliamentary answer, digital-arrest-related reports; NPCI, UPI activity; and official legal publications, statutory and capacity information. Secondary studies provide context, not replacement national counts. Unclear periods or denominators are flagged.

### D. Data Collection Tool

For each source, the extraction recorded its period, unit, reporting process and whether it measured complaints, registered cases, incidents, transactions, reported amounts, lien/saved amounts or outcomes. Analysis is descriptive: endpoint ratios and year-on-year changes are calculated only within a series; no inferential tests, causal models or case-level estimates are used. Definitions are not pooled and missing values are not imputed. Legal mapping matches described conduct to potentially relevant statutory elements, evidence and institutional responsibilities.

### Dataset Coverage and Comparability

The datasets are not merged. Table 2 distinguishes registered cases, complaints, digital-arrest-related NCRP reports and UPI activity. Unverifiable fraud-enablement percentages are excluded. Complaints are not equivalent to FIRs, convictions or confirmed unrecovered losses.

**Table 2:** Dataset Coverage and Interpretation

| Dataset | Period used | What it measures and key limitation |
|---|---|---|
| NCRB | 2014–2024 | Police-registered cybercrime cases; does not capture all unreported incidents. |
| NCRP/CFCFRMS | 2021–2025 | Financial-fraud complaints and amounts reported by complainants; not a count of FIRs or verified final losses. |
| NCRP digital-arrest-related reports | 2022–2024 | Incidents and defrauded amounts for the combined category of digital-arrest scams and related cybercrimes; not a standalone NCRB series. |
| NPCI UPI statistics | FY2021–22 to FY2025–26 | Annual UPI transaction volume and value; these are payment-activity measures, not fraud measures. |

*Note: FY2025–26 is a completed financial year in the official NPCI-derived table cited here. UPI activity is kept separate from cybercrime and financial-fraud complaints.*

### E. Variables Used

The principal variables are year/reference period, State/UT, registered cybercrime cases, NCRP financial-fraud complaints, reported amount, NCRP-reported digital-arrest scams and related cybercrimes and amounts, UPI transaction volume/value, published indicators of FIRs, charge sheets, convictions, forensic assistance and funds marked as lien or returned. The variables are not interchangeable: complaints are not necessarily FIRs, a reported amount is not a verified final loss, and a lien or saved amount is not automatically a refund to a victim. Regional rates adjusted by population or internet users are not calculated because a consistent matched denominator was not included in the extracted source set; absolute counts are therefore described as registration totals only.

### F. Ethical Considerations

The study uses public secondary data, with no human participants or personal case records. Sources are cited and reported figures are not presented as verified individual outcomes.

### G. Limitations

The study has no interviews, victim surveys, police files or case-level cohort tracking. Its sources cover different periods and reporting processes; UPI figures are from the official NPCI-derived release. Under-reporting is unobserved, complaints are not linked through court outcomes or refunds, and matched State population/internet-user denominators are unavailable. Findings are descriptive and cannot establish causation or conclusively measure legal effectiveness.

## 4. Data Analysis

### A. National Cybercrime Trend in India

The NCRB data show a substantial increase in registered cybercrime cases in India from 9,622 in 2014 to 101,928 in 2024. The 2014–2023 series is taken from the MHA's Lok Sabha answer of 2 December 2025, and the 2024 endpoint from the MHA's July 2026 update [5], [22]. The increase was not uniform: notable year-on-year rises occurred in 2017 and 2019, while growth was lower in 2021. Cases then increased from 65,893 in 2022 to 86,420 in 2023 and 101,928 in 2024.

These are police-registered cases, not a count of all offences; reporting and registration practices affect recorded totals.

**Table 3:** NCRB-Registered Cybercrime Cases, 2014–2024 [5], [22]

| Year | Cases | YoY |
|---|---|---|
| 2014 | 9,622 | — |
| 2015 | 11,592 | +20.5% |
| 2016 | 12,317 | +6.3% |
| 2017 | 21,796 | +77.0% |
| 2018 | 27,248 | +25.0% |
| 2019 | 44,735 | +64.2% |
| 2020 | 50,035 | +11.8% |
| 2021 | 52,974 | +5.9% |
| 2022 | 65,893 | +24.4% |
| 2023 | 86,420 | +31.2% |
| 2024 | 101,928 | +18.0% |

Note: Year-on-year percentages are calculated from the reported annual totals and rounded to one decimal place.

### B. State-wise Distribution of Registered Cybercrime Cases

The 2024 State-wise data show substantial variation in registered cybercrime cases. Among States (excluding Union Territories), Telangana recorded the highest total at 27,230, followed by Karnataka (21,993), Uttar Pradesh (11,073), Maharashtra (9,922) and Bihar (6,380). Table 4 presents the 15 States with the highest registered totals. These are absolute counts, not population-adjusted risk estimates.

State totals reflect population, internet access, digital adoption and reporting practices as well as offending. They show where more cases were registered, not individual risk. Population- or internet-user-adjusted comparison is not possible without matched denominators; no causal explanation is inferred.

**Table 4:** 15 States with the Highest Registered Cybercrime Totals, 2024 [22]

| State | Cases |
|---|---|
| Telangana | 27,230 |
| Karnataka | 21,993 |
| Uttar Pradesh | 11,073 |
| Maharashtra | 9,922 |
| Bihar | 6,380 |
| Tamil Nadu | 5,793 |
| Kerala | 2,962 |
| Andhra Pradesh | 2,528 |
| Odisha | 2,501 |
| Haryana | 1,815 |
| Gujarat | 1,592 |
| Rajasthan | 1,527 |
| Jharkhand | 1,423 |
| Madhya Pradesh | 1,081 |
| Punjab | 888 |

Note: Union Territories are excluded from this State-only ranking. Absolute registered totals are not population-adjusted rates.

### C. NCRP Financial-Fraud Complaint Trends

NCRP measures complaints reported through the national cybercrime reporting system, which differs from NCRB's measure of police-registered cases. Financial-fraud complaints increased from 262,846 in 2021 to 2,402,579 in 2025. The corresponding reported amount increased from Rs.551 crore to Rs.22,495 crore.

These amounts represent financial exposure reported through complaints, not necessarily

the final loss suffered by victims or the amount ultimately unrecovered. Complaints rose by approximately 9.1 times between 2021 and 2025. The reported amount peaked at Rs.22,848 crore in 2024 and was Rs.22,495 crore in 2025, about 1.5% lower, even as the number of complaints continued to rise. This divergence shows why complaint volume and reported financial amount should be analysed separately; the aggregate figures alone do not explain the change in average reported amount or establish how much was ultimately recovered. Investigation, fund marking, recovery and legal action occur after reporting and involve the relevant authorities. A separate MHA update reported that, for 2021–2025, more than 6.58 million financial-fraud complaints had been received, more than Rs.55,050 crore had been reported, more than Rs.8,189 crore had been marked as lien, and more than 195,760 FIRs had been registered. It also reported that more than Rs.11,158 crore had been saved through CFCFRMS in over 32.80 lakh complaints by 30 June 2026 [22]. These are aggregate administrative indicators with different operational meanings and cut-off dates; they cannot be divided into a complaint-to-FIR conversion rate or treated as proof that the stated amounts were all returned to victims.

**Table 5:** NCRP Financial-Fraud Complaints and Reported Amount [7]

| Year | Complaints | Amount reported |
|---|---|---|
| 2021 | 262,846 | Rs.551 crore |
| 2022 | 694,446 | Rs.2,290 crore |
| 2023 | 1,310,357 | Rs.7,465 crore |
| 2024 | 1,918,835 | Rs.22,848 crore |
| 2025 | 2,402,579 | Rs.22,495 crore |

Note: NCRP/CFCFRMS data are dynamic; amounts reported by complainants are not equivalent to verified final losses or amounts ultimately returned.

### D. Digital-Arrest-Related Reports and Defrauded Amounts

The Ministry of Home Affairs' parliamentary answer reported 39,925 incidents and Rs.91.14 crore in defrauded amount in 2022, 60,676 incidents and Rs.339.03 crore in 2023, and 123,672 incidents and Rs.1,935.51 crore in 2024 for the combined category 'digital-arrest scams and related cybercrimes' reported on NCRP [13]. The source labels the monetary column as a defrauded amount; these are portal reports, not NCRB registered-case totals, a standalone digital-arrest series, or independently verified final losses. The incident count increased about 3.1-fold and the reported defrauded amount about 21.2-fold between 2022 and 2024. These comparisons describe the reported series only; they do not by themselves show investigation success, conviction rates or how much money was returned.

**Table 6:** NCRP-Reported Digital-Arrest Scams and Related Cybercrimes [13]

| Year | Incidents | Defrauded amount |
|---|---|---|
| 2022 | 39,925 | Rs.91.14 crore |
| 2023 | 60,676 | Rs.339.03 crore |
| 2024 | 123,672 | Rs.1,935.51 crore |

Note: The parliamentary category combines digital-arrest scams and related cybercrimes reported on NCRP; it is not a separate NCRB count of digital-arrest offences.

### E. UPI Growth and Payment-System Context

UPI transaction value rose from Rs.84.16 lakh crore in FY2021–22 to Rs.314.23 lakh crore in FY2025–26, while annual transaction volume rose from 4,595.61 crore to 24,161.69 crore transactions. These official NPCI-derived totals document growth in UPI usage, but do not establish that payment growth caused an increase in fraud. This paper does not calculate a UPI fraud rate because a consistent, independently verified UPI-only fraud series with a matching definition and denominator was not available in the source material.

**Table 7:** UPI Transactions in India, FY2021–22 to FY2025–26 [8]

| FY | Volume (crore transactions) | Value (Rs. lakh crore) |
|---|---|---|
| 2021–22 | 4,595.61 | 84.16 |
| 2022–23 | 8,371.44 | 139.15 |
| 2023–24 | 13,112.95 | 199.95 |
| 2024–25 | 18,586.60 | 260.56 |
| 2025–26 | 24,161.69 | 314.23 |

### F. Fraud Enablement Methods

Phishing, vishing, collect-request misuse and remote-access application misuse are distinct mechanisms that may overlap within a single incident. Because the percentages supplied in the earlier draft could not be traced to a source with a verifiable sample, denominator and observation period, they are excluded from quantitative comparison and are not used to rank national prevalence.

### G. Comparative Analysis of Cybercrime and Digital-Fraud Indicators

The datasets measure different processes. NCRB records police-registered cybercrime cases; NCRP records complaints submitted through the national reporting system; UPI data describes payment activity; and the digital-arrest series represents NCRP-reported digital-arrest scams

and related cybercrimes. They provide complementary indicators and should not be combined into a single total of cybercrime.

Within each series, NCRB registrations rose about 10.6-fold between 2014 and 2024 and NCRP financial-fraud complaints about 9.1-fold between 2021 and 2025 [5], [7], [22]. These series are not directly comparable, and growth may reflect reporting and registration changes as well as offending. UPI volume and value increased about 5.3-fold and 3.7-fold respectively between FY2021–22 and FY2025–26; this measures payment-system growth, not fraud incidence [8]. NCRP's reported amount fell about 1.5% from 2024 to 2025 despite rising complaints [7]. Report counts, reported amounts, lien-marked funds and refunds are distinct indicators.

Complaints do not necessarily become FIRs or prosecutions. Future evaluation should track matched cohorts from complaint to investigation, charge sheet, trial and outcome, while separately reporting funds frozen, saved and actually returned.

**Table 8:** Comparison of Major Data Indicators

| Indicator | Measures | Period |
|---|---|---|
| NCRB cases | Police-registered cybercrime | 2014–2024 |
| NCRP financial fraud | Reported financial-fraud complaints | 2021–2025 |
| Digital-arrest-related NCRP reports | Combined incidents and defrauded amounts | 2022–2024 |
| UPI activity | Payment transaction volume and value | FY2021–22–FY2025–26 |

### H. Key Findings

The indicators show growth in registered cases, financial-fraud complaints and digital-arrest-related NCRP reports. State totals are not population-adjusted, and UPI activity is not a fraud measure. The evidence describes reporting patterns, not underlying prevalence or causation; aggregate sources do not link complaints through the full justice process.

## 5. Discussion

The indicators are not directly comparable and may reflect offending, digital adoption, awareness and registration practices. Reported financial amounts fell slightly in 2025 despite rising complaints; aggregate data do not explain the divergence or establish final unrecovered losses [7]. Telangana and Karnataka recorded the highest absolute State totals, but these are not population-adjusted risk rates [22]. Digital-arrest-related reports rose sharply from 2022 to 2024, yet do not reveal investigation success or funds recovered [13]. UPI growth describes payment activity, not fraud [8]. India's framework is complementary: the IT Act addresses

cyber-specific offences, BNS provisions may address cheating or personation, the BSA governs electronic evidence, CERT-In Directions impose specified incident duties, and the DPDP framework applies according to its commencement schedule. The existence of these instruments does not demonstrate effective enforcement. Evidence is distributed across devices, banks, telecom providers and platforms; timely preservation, provenance and coordination are essential. National support and forensic facilities exist [20]–[22], but the reviewed aggregate data do not establish equal access or improved court outcomes. The defensible conclusion is therefore qualified: India has a multi-layered framework, but public data do not yet permit a robust assessment of its effectiveness.

## 6. Legal and Institutional Implications

The mapping is illustrative, not a claim that one statute applies automatically. The offence and procedure depend on the facts and evidence; the table identifies potentially relevant provisions and investigative needs.

**Table 9:** Illustrative Mapping of Fraud Typologies to Legal and Investigative Requirements

| Fraud typology | Potentially relevant framework | Investigative and evidentiary issue |
|---|---|---|
| Identity theft or account takeover | IT Act, Section 66C; other provisions may apply depending on conduct | Establish how credentials or identifiers were obtained and used; preserve access logs, device artefacts and account records. |
| Impersonation and digital-arrest scams | IT Act, Section 66D; BNS Sections 318(4) and 319 may be relevant where their elements are met | Correlate calls, messages, account identifiers, transfer trails and impersonated identities across service providers and jurisdictions. |
| Phishing, malicious links or unauthorised access | IT Act provisions, including Sections 43 and 66 where their statutory elements are met; other offences may apply | Preserve messages, headers, URLs, device artefacts and provider records; distinguish a deceptive attempt from a proven system intrusion. |
| Electronic records used in prosecution | Bharatiya Sakshya Adhiniyam, 2023, including Section 63 and its requirements | Maintain provenance, integrity, lawful collection records and applicable certification requirements for electronic records. |
| Reportable cybersecurity incidents and log retention | Applicable CERT-In Directions and sector-specific requirements | Determine whether a reporting obligation applies, document timelines and retain relevant logs in accordance with applicable requirements. |
| Personal-data processing or breach issues | Digital Personal Data Protection Act, 2023 and applicable rules, when their scope and commencement provisions apply | Establish the data-processing relationship and applicable obligations; the DPDP framework should not be treated as a general substitute for criminal offences. |

## Implications for Practice and Policy

Policy priorities are consistent reporting definitions; complaint-to-outcome cohort tracking; investigation-time measures; separate reporting of lien, frozen, saved and refunded funds; and population-adjusted regional comparisons. Forensic assessment should measure staffing, caseload, turnaround time and State/UT access. These are evaluation priorities, not proven causal solutions.

## 7. Conclusion

This study combines doctrinal review with descriptive analysis of public secondary data. NCRB cases rose from 9,622 in 2014 to 101,928 in 2024, while NCRP financial-fraud complaints rose from 262,846 in 2021 to 2,402,579 in 2025; these are distinct reporting measures. The typology–provision–capacity mapping links selected fraud methods to potentially relevant laws, evidence and institutional responsibilities. Rising reports do not prove legal failure, and the existence of laws does not prove effective enforcement. Further research should track matched cohorts from complaint to court outcome and distinguish reported, restrained and returned funds. Because this study uses aggregate data and no case-level records, India's overall response effectiveness remains unresolved and requires outcome-based evaluation.

## References


1. Government of India, *Information Technology Act, 2000*, Act No. 21 of 2000, India Code. Available: https://www.indiacode.nic.in/indiacode/handle/123456789/1999.
2. Government of India, *Bharatiya Nyaya Sanhita, 2023*, Act No. 45 of 2023, effective 1 July 2024, India Code. Available: https://www.indiacode.nic.in/indiacode/handle/123456789/20062.
3. Government of India, *Digital Personal Data Protection Act, 2023*, Act No. 22 of 2023, India Code. Available: https://www.indiacode.nic.in/indiacode/handle/123456789/22037.
4. Ministry of Electronics and Information Technology, Government of India, *Digital Personal Data Protection Rules, 2025*, G.S.R. 846(E), Gazette of India, 13 November 2025; staged commencement under Rule 1. Available: https://www.meity.gov.in/static/uploads/2025/11/53450e6e5dc0bfa85ebd78686cadad39.pdf.
5. Ministry of Home Affairs, Government of India, "Rise in Cybercrime Cases," Lok Sabha Unstarred Question No. 438, 2 December 2025, Annexure I (crime-head totals, 2014–2023). Available: https://www.mha.gov.in/MHA1/Par2017/pdfs/par2025-pdfs/LS02122025/438.pdf.
6. S. S. Tripathy, "A Comprehensive Survey of Cybercrimes in India Over the Last Decade," *International Journal of Science and Research Archive*, vol. 13, no. 1, pp. 2360–2374, 2024. doi: 10.30574/ijsra.2024.13.1.1919. Available: https://ijsra.net/sites/default/files/IJSRA-2024-1919.pdf.
7. Ministry of Home Affairs, Government of India, "Cyber Crime Reporting and Investigation," Press Information Bureau, 11 February 2026. Available: https://www.pib.gov.in/PressReleasePage.aspx?PRID=2226441.
8. Ministry of Finance, Government of India, "Nearly 55.49 Crore Users Onboarded on UPI as in June 2026," Press Information Bureau, 20 July 2026. Includes the NPCI-derived table "UPI transactions during the last five financial years." Available: https://www.pib.gov.in/PressReleaseIframePage.aspx?PRID=2286608.
9. Reserve Bank of India, *Annual Report 2023–24*, Mumbai, 2024. Available: https://www.rbi.org.in/Scripts/AnnualReportPublications.aspx?Id=1399.
10. I. V. S. Panwar and P. Shekhar, "The Rise of Digital Arrests in India: An In-Depth Exploration of Unlawful Cyber Detentions and Criminological Countermeasures," *International Journal for Multidisciplinary Research*, vol. 7, no. 5, 2025. doi: 10.36948/ijfmr.2025.v07i05.55866. Available: https://www.ijfmr.com/research-paper.php?id=55866.
11. K. Rani, "Cybercrime and Legal Responses in the Indian Jurisdiction," *Indian Journal of Law*, vol. 1, no. 1, pp. 35–41, 2023. doi: 10.36676/ijl.2023-v1i1-05. Available: https://law.shodhsagar.com/index.php/j/article/view/5.
12. P. Dandotiya and H. Veer, "Preventing Cybercrime in India: A Critical Analysis of Legal Frameworks and Enforcement Mechanisms," *International Journal of Research & Technology*, vol. 13, no. 4, pp. 971–986, 2025. doi: 10.64882/ijrt.v13.i4.914. Available: https://ijrt.org/j/article/view/914.
13. Ministry of Home Affairs, Government of India, "Combating Digital Arrest, Blackmail, and Cyber Impersonation of Law Enforcement Agencies," Rajya Sabha Unstarred Question No. 1505, 12 March 2025. Available: https://www.mha.gov.in/MHA1/Par2017/pdfs/par2025-pdfs/RS12032025/1505.pdf. The reported incident and loss figures are reproduced as stated in the parliamentary answer.
14. Federal Communications Commission, "Protecting Consumers from SIM Swap and Port-Out Fraud," FCC 23-95, 2023. Available: https://docs.fcc.gov/public/attachments/FCC-23-95A1_Rcd.pdf.

15. Cybersecurity and Infrastructure Security Agency, "Recognize and Report Phishing," U.S. Department of Homeland Security. Available: https://www.cisa.gov/secure-our-world/recognize-and-report-phishing.
16. National Institute of Standards and Technology, *Frontier Research on Mitigating Risks from Synthetic Content: A Call to Action*, U.S. Department of Commerce, 2024. Available: https://www.nist.gov/caissi/frontier-research-mitigating-risks-synthetic-content-call-action.
17. Federal Bureau of Investigation, "Senior U.S. Officials Impersonated in Malicious Messaging Campaign," 2025. Available: https://www.fbi.gov/investigate/cyber/alerts/2025/senior-us-officials-impersonated-in-malicious-messaging-campaign.
18. Indian Computer Emergency Response Team (CERT-In), *Directions under sub-section (6) of section 70B of the Information Technology Act, 2000*, 28 April 2022. Available: https://www.cert-in.org.in/Directions70B.jsp.
19. Indian Computer Emergency Response Team (CERT-In), official FAQs and clarifications concerning the 2022 Directions. Available: https://www.cert-in.org.in/PDF/FAQs_on_CyberSecurityDirections_May2022.pdf.
20. Ministry of Home Affairs, Government of India, "Forensic Labs," Press Information Bureau, 18 December 2024. Available: https://www.pib.gov.in/PressReleasePage.aspx?PRID=2085688.
21. Ministry of Home Affairs, Government of India, *Annual Report 2024–25*, 2026. Available: https://www.mha.gov.in/sites/default/files/AREnglish_24032026.pdf.
22. Ministry of Home Affairs, Government of India, "National Cyber Crime Data," Press Information Bureau, 21 July 2026. Available: https://www.pib.gov.in/PressReleasePage.aspx?PRID=2287039.
23. Government of India, *Bharatiya Sakshya Adhiniyam, 2023*, Act No. 47 of 2023, effective 1 July 2024, India Code. Available: https://www.indiacode.nic.in/indiacode/handle/123456789/20063.
24. Ministry of Home Affairs, Government of India, "Digital Arrest Scam," Press Information Bureau, 10 December 2024. Available: https://www.pib.gov.in/Pressreleaseshare.aspx?PRID=2082761.
25. Ministry of Electronics and Information Technology, Government of India, "Commencement Notification under the Digital Personal Data Protection Act, 2023," G.S.R. 843(E), Gazette of India, 13 November 2025. Available: https://egazette.gov.in/WriteReadData/2025/267647.pdf.
26. N. Narena and K. Gupta, "Rethinking India's cybercrime law: from information technology act to emerging threats in a global context," *International Review of Law, Computers & Technology*, published online 15 May 2026. doi: 10.1080/13600869.2026.2668321. Available: https://doi.org/10.1080/13600869.2026.2668321.
27. T. K. Biswas, "Data and information theft in e-commerce, jurisdictional challenges, related issues and response of Indian laws," *Computer Law & Security Review*, vol. 27, no. 4, pp. 385–393, 2011. doi: 10.1016/j.clsr.2011.05.009. Available: https://doi.org/10.1016/j.clsr.2011.05.009.
28. Indian Cyber Crime Coordination Centre (I4C), National Cybercrime Threat Analytics Unit, "Digital Arrest Scam," Advisory TAU/ADV/003, 6 March 2025. Available: https://cybercrime.gov.in/pdf/Advisories/ADVISORYTAU-ADV-003DigitalArrest06.03.2025.pdf.