



KAMARAJ IAS ACADEMY
Only IAS Academy by Grandson of "Perunthalaivar Kamarajar"

Cybercrime in India Rises Despite Overall Crime Decline, Exposing New Challenges for Digital Governance and Internal Security

Published On: 03-10-2026

Recent Developments:

- The **NCRB Crime in India 2024 Report** recorded **58.85–58.86 lakh cognisable crimes** in 2024, compared with 62.41 lakh in 2023, representing an overall decline of about **6%**; the crime rate fell from **448.3 to 418.9 cases per lakh population**.
- In contrast, registered **cybercrime cases crossed one lakh in 2024**, rising by about **17%** from 86,420 cases in 2023. Financial fraud constituted the dominant category, accounting for around **72.6%** of reported cybercrime cases.
- The contrasting trends indicate a structural shift in the crime landscape: conventional registered crime declined, while **digitally enabled financial fraud, impersonation and cyber-enabled deception** expanded rapidly.
- The Ministry of Home Affairs has identified the **Indian Cyber Crime Coordination Centre (I4C)** and the **National Cyber Crime Reporting Portal (NCRP)** as major components of India's coordinated response to cybercrime.
- The **Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Amendment Rules, 2026** strengthened regulation of synthetically generated information, including deepfakes, and reduced the compliance period for removal of unlawful content following specified government or court orders from 36 hours to **3 hours**.
- The **Digital Personal Data Protection Rules, 2025** were notified by MeitY in November 2025, providing the implementation framework for the Digital Personal Data Protection Act, 2023 through a phased compliance structure.

Understanding Cybercrime:

Meaning and Scope:

- **Cybercrime** refers to criminal activity in which computers, communication networks, digital devices or information systems are used as the **target, medium or instrument** of an offence.
- Cybercrime includes activities such as **identity theft, online financial fraud, phishing, ransomware, cyberstalking, hacking, impersonation, data theft, cyber extortion and cyber terrorism**.
- Cybercriminals exploit vulnerabilities in digital infrastructure as well as weaknesses in human behaviour, organisational processes and institutional systems.
- The contemporary cybercrime ecosystem therefore combines **technical exploitation with social engineering**, making cybersecurity both a technological and governance challenge.

Changing Nature of Cybercrime:

Kamaraj IAS Academy

Plot A P.127, AF block, 6 th street, 11th Main Rd, Shanthi Colony, Anna Nagar, Chennai, Tamil Nadu 600040

Phone: **044 4353 9988 / 98403 94477 / Whatsapp : 09710729833**

- Traditional cyberattacks often depended heavily on technical vulnerabilities, whereas contemporary scams increasingly exploit **trust, fear, urgency and institutional credibility**.
- Common examples include fake delivery calls, fraudulent investment schemes, impersonation of bank officials, fake police or government calls, and claims that a person's mobile number has been linked to illegal activities.
- **Digital Arrest scams** illustrate this shift particularly clearly: fraudsters impersonate police officers or other authorities, create fear of arrest and demand immediate payments.
- Investment scams exploit the aspiration for **quick financial returns**, delivery scams exploit trust in e-commerce, bank impersonation exploits institutional credibility, while fake police calls exploit fear of authority.
- The core lesson is that cybersecurity cannot be addressed only through stronger encryption or firewalls; **human behaviour and social engineering** have become central attack surfaces.

Major Forms of Cybercrime:

Financial Cybercrime:

- Financial cybercrime includes **UPI fraud, phishing, card fraud, internet-banking fraud, investment scams, loan scams, mule-account operations and fraudulent payment requests**.
- The rapid nature of digital payment systems allows fraudsters to transfer money through multiple accounts before victims or banks can intervene.
- The government's **Citizen Financial Cyber Fraud Reporting and Management System (CFCFRMS)** seeks to enable rapid reporting and coordination with banks and financial institutions to prevent further siphoning of funds.

Identity and Impersonation Crimes:

- Criminals obtain personal information such as **mobile numbers, Aadhaar-related information, bank details, passwords and login credentials** and use them to impersonate victims or trusted institutions.
- Section **66C of the Information Technology Act, 2000** addresses identity theft, while Section **66D** deals with cheating by personation using computer resources or communication devices.

Deepfakes and Synthetic Media:

- Artificial intelligence has lowered the cost of producing convincing **synthetic audio, video and visual content**.
- Deepfakes can facilitate impersonation, financial fraud, misinformation, reputational harm, non-consensual intimate imagery and other unlawful activities.
- The 2026 IT Rules framework requires platforms to undertake technical measures against unlawful synthetic content and provides for **labelling and traceability mechanisms** for permissible synthetic content.

Impact of Cybercrime:

National Security:

- Cyberattacks against **critical infrastructure, defence networks, government systems, telecommunications and financial infrastructure** can create consequences extending beyond individual victims.
- State-sponsored actors and organised criminal groups can exploit cyber vulnerabilities for espionage, disruption, financial gain or strategic coercion.

Economic and Financial Losses:

- Cyber fraud directly affects individuals, banks, businesses and governments through **unauthorised transfers, ransomware, payment fraud and data theft**.

- Large-scale financial fraud also imposes indirect costs through investigation, dispute resolution, cybersecurity investments and loss of consumer confidence.

Data and Privacy Risks:

- Data breaches can expose **personal information, intellectual property, trade secrets and confidential institutional information**.
- The expansion of digital public services makes protection of personal data essential for maintaining trust in the digital economy.

Disruption of Essential Services:

- Cyberattacks can disrupt **power systems, transportation, telecommunications, banking and public services**.
- Greater digital dependence therefore increases the potential systemic impact of a successful cyberattack.

Erosion of Trust:

- Repeated cyber fraud can weaken public confidence in **digital payments, online banking, e-governance and digital public infrastructure**.
- This creates a governance paradox: digitalisation improves accessibility and efficiency, but inadequate cybersecurity can reduce public willingness to use digital services.

Major Challenges in Tackling Cybercrime:

Technology–Law Enforcement Gap:

- Cybercriminals can rapidly adopt **deepfakes, spoofing, encryption, virtual private networks, automated fraud tools and cryptocurrency-related techniques**, while investigative capacity often develops more slowly.
- Attribution becomes difficult when offenders, victims, servers, financial accounts and digital infrastructure are located across different jurisdictions.

Social Engineering:

- Modern fraud increasingly succeeds without sophisticated hacking because criminals manipulate victims into **sharing credentials, installing malicious applications or authorising transactions themselves**.
- Fear, urgency and impersonation are particularly effective against vulnerable or less digitally literate users.

Speed of Digital Payments:

- Instant payment systems provide major economic benefits but also reduce the time available for intervention after fraudulent transactions.
- The effectiveness of cyber-fraud prevention therefore depends heavily on **real-time detection, rapid reporting and immediate financial coordination**.

Under-Reporting and Delayed Reporting:

- Victims may delay reporting because of **embarrassment, fear, social stigma or uncertainty about where to complain**.
- Delay reduces the possibility of freezing or recovering transferred funds.

Forensic Capacity:

- Cybercrime investigations require specialised expertise in **digital forensics, malware analysis, device extraction, blockchain tracing, electronic evidence preservation and cyber attribution**.
- Uneven capacity across police stations and States can affect investigation quality and prosecution.

Jurisdictional Fragmentation:

- **Police and public order are State subjects**, making State and Union Territory law-enforcement agencies primarily responsible for prevention, investigation and prosecution of cybercrime.
- Cybercrime, however, routinely crosses State and national boundaries, creating a mismatch between the **territorial structure of policing and the borderless nature of cyberspace**.

Constitutional Foundations of Cyber Governance:

Article 21 — Right to Life, Liberty and Privacy:

- In **K.S. Puttaswamy v. Union of India (2017)**, the Supreme Court recognised the **Right to Privacy as a fundamental right** derived from Article 21 and other constitutional guarantees.
- Privacy principles are directly relevant to **data protection, surveillance, collection of personal information, data breaches and state use of digital technologies**.
- Cyber governance must therefore balance legitimate security objectives with constitutional requirements of **legality, necessity and proportionality**.

Article 19(1)(a) — Freedom of Speech and Expression:

- Digital platforms have become major spaces for **political, social, educational and commercial expression**.
- In **Shreya Singhal v. Union of India (2015)**, the Supreme Court struck down Section 66A of the IT Act because its vague and overbroad restrictions on online speech were inconsistent with Article 19(1)(a).
- The judgment remains important for understanding the constitutional limits of regulating online expression.

Article 19(2) — Reasonable Restrictions:

- Digital speech may be regulated through constitutionally permitted restrictions relating to grounds such as **sovereignty and integrity of India, security of the State and public order**.
- Cyber regulation therefore requires a balance between preventing unlawful digital activity and protecting legitimate online expression.

Legislative Distribution:

- **Police and public order** fall under the State List, making States and Union Territories primarily responsible for criminal investigation and prosecution.
- At the same time, **information technology** is substantially governed through Union legislation, including Parliament's competence under its constitutional powers.
- This creates a distinctive federal challenge in which **cybercrime is locally investigated but frequently technologically and geographically transnational**.

Primary Statutory Framework:

Information Technology Act, 2000:

- The **Information Technology Act, 2000**, amended substantially in 2008, remains the principal legislation dealing specifically with electronic records, digital transactions, intermediary responsibilities and several cyber offences.
- **Section 43** provides for penalties and compensation for unauthorised damage to computers, computer systems and related resources.

- **Section 43A** provides for compensation in specified circumstances involving failure of a body corporate to implement reasonable security practices for sensitive personal data.
- **Section 66** deals with computer-related offences committed with the requisite dishonest or fraudulent intent.
- **Sections 66C and 66D** address identity theft and cheating by personation using computer resources or communication devices.
- **Section 66F** deals with cyber terrorism and provides for punishment extending to **imprisonment for life**.
- **Section 69A** empowers the Central Government to direct blocking of public access to information in specified circumstances and subject to the statutory procedure.
- The Act also provides the statutory foundation for **CERT-In** under Section 70B and the protection framework for critical information infrastructure through Section 70A.

Information Technology Rules, 2026:

- The 2026 amendments strengthened intermediary obligations concerning **synthetically generated information**, including deepfakes and AI-generated content.
- Platforms are required to undertake reasonable technical measures against unlawful synthetic content and ensure appropriate identification or labelling of permissible synthetic material.
- For specified government or court orders concerning unlawful information, the removal timeline was reduced from **36 hours to 3 hours**.
- The framework also strengthens requirements concerning harmful synthetic content involving **impersonation, child sexual exploitation, non-consensual intimate imagery and deceptive material**.

Digital Personal Data Protection Act, 2023:

- The **Digital Personal Data Protection Act, 2023** establishes a framework for processing digital personal data while recognising individual rights and legitimate purposes for data processing.
- It introduces obligations for **Data Fiduciaries**, provides rights to individuals and establishes institutional mechanisms for data-protection enforcement.
- The **Digital Personal Data Protection Rules, 2025**, notified in November 2025, provide the operational framework for implementation, with several provisions subject to a phased commencement structure.
- The framework complements criminal law by addressing the **governance and protection of personal data**, rather than functioning solely as a cybercrime punishment statute.

Bharatiya Nyaya Sanhita, 2023 and Bharatiya Sakshya Adhiniyam, 2023:

- The **Bharatiya Nyaya Sanhita (BNS), 2023** replaced the Indian Penal Code and provides the broader criminal-law framework applicable to offences that may involve digital technologies.
- The **Bharatiya Sakshya Adhiniyam (BSA), 2023** replaced the Indian Evidence Act and provides the contemporary evidentiary framework for electronic and digital records.
- **Section 63 of the BSA** addresses admissibility requirements for electronic records and incorporates mechanisms relating to certification and identification of digital records.
- The statutory schedule includes details such as the relevant **device or digital source and hash values**, strengthening the evidentiary chain for electronic records.

Institutional Governance Architecture:

CERT-In:

- The **Indian Computer Emergency Response Team (CERT-In)** is the national nodal agency for responding to cybersecurity incidents under **Section 70B of the IT Act**.
- It performs functions relating to incident response, cybersecurity advisories, vulnerability information, coordination and strengthening the resilience of India's cyber infrastructure.
- CERT-In operates primarily within the **technical and cybersecurity incident-response domain**.

I4C:

- The **Indian Cyber Crime Coordination Centre (I4C)** functions under the Ministry of Home Affairs as a central institutional mechanism for coordinated action against cybercrime.
- It provides an operational framework connecting **law-enforcement agencies, financial institutions, forensic institutions and other stakeholders.**
- The I4C also operates the **National Cyber Crime Reporting Portal** and the **1930 helpline.**

National Cyber Crime Reporting Portal:

- The **National Cyber Crime Reporting Portal** enables citizens to report cybercrime incidents, including offences against women and children.
- The **1930 helpline** provides a rapid channel for reporting financial cyber fraud.
- Early reporting is crucial because intervention during the initial transaction chain can improve the possibility of **freezing and recovering defrauded funds.**

CFCFRMS:

- The **Citizen Financial Cyber Fraud Reporting and Management System** facilitates immediate reporting and coordination between law-enforcement agencies and financial institutions.
- By June 2026, the system had reportedly helped save more than **₹11,158 crore** across over **32.80 lakh complaints**, according to the Ministry of Home Affairs.
- The 2026 Standard Operating Procedure for NCRP-CFCFRMS further standardised **complaint processing, bank coordination, grievance redressal, lien removal and restoration of defrauded funds.**

NCIIPC:

- The **National Critical Information Infrastructure Protection Centre (NCIIPC)** functions under Section 70A of the IT Act.
- It focuses on protecting **Critical Information Infrastructure (CII)** whose disruption or destruction could have a debilitating impact on national security, economy, public health or safety.
- Its role is distinct from CERT-In: **CERT-In focuses broadly on cybersecurity incident response, while NCIIPC focuses specifically on critical information infrastructure protection.**

Cyber Forensics:

- The government has established specialised cyber-forensic facilities to support State and Union Territory police.
- The **National-Digital Investigation Support Centre**, functioning under I4C, provides early-stage cyber-forensic assistance to investigating officers, while the National Cyber Forensic Laboratory at Hyderabad supports evidentiary examination.

National Crime Records Bureau:

Establishment and Mandate:

- The **National Crime Records Bureau (NCRB)** was established in **1986** under the Ministry of Home Affairs.
- Its creation was associated with recommendations of the **Tandon Committee, National Police Commission and the Ministry of Home Affairs Task Force.**
- **Headquarters:** New Delhi.
- NCRB serves as the national repository and analytical institution for crime and criminal statistics.

Major Functions:

Kamaraj IAS Academy

Plot A P.127, AF block, 6 th street, 11th Main Rd, Shanthi Colony, Anna Nagar, Chennai, Tamil Nadu 600040

Phone: **044 4353 9988 / 98403 94477 / Whatsapp : 09710729833**

- NCRB **collects, compiles and analyses crime data** to support investigation, policymaking and criminal-justice administration.
- It publishes major statistical reports including **Crime in India, Accidental Deaths and Suicides in India, and Prison Statistics India**.
- NCRB coordinates and monitors the **Crime and Criminal Tracking Network and Systems (CCTNS)** project.
- Through the **National Digital Police Portal**, authorised police personnel can access criminal and investigative information available through connected databases.
- NCRB maintains the **National Database of Sexual Offenders** and facilitates information sharing with States and Union Territories.
- It manages technical and operational functions associated with cybercrime reporting mechanisms and supports cybercrime investigation through training initiatives such as **CyTrain**.
- The **Central Finger Print Bureau** functions under NCRB and serves as a national repository and coordinating institution for fingerprint information.

Critical Analytical Issues for UPSC Mains:

From Cybersecurity to Cyber Justice:

- India's challenge is no longer limited to preventing cyberattacks; it also involves ensuring **rapid reporting, effective investigation, electronic evidence management, prosecution, adjudication and victim compensation**.
- Cyber justice requires the complete chain from **incident detection ? complaint registration ? fund freezing ? forensic investigation ? electronic evidence preservation ? prosecution ? recovery and restitution**.

Federalism versus Borderless Crime:

- Cybercrime requires coordination across States, financial institutions, technology companies and foreign jurisdictions.
- Strengthening **inter-State Joint Cyber Coordination Teams**, common investigative protocols and interoperable databases can reduce jurisdictional fragmentation.

Human-Centric Cybersecurity:

- Since social engineering is increasingly important, cybersecurity policy must combine technology with **digital literacy, behavioural awareness and institutional authentication protocols**.
- Citizens should be trained to recognise urgency-based requests, unsolicited investment offers, fake authority calls and suspicious payment demands.

International Cooperation:

- Cybercrime frequently involves foreign servers, foreign intermediaries and transnational criminal networks.
- India therefore needs stronger **mutual legal assistance, expedited electronic-evidence sharing, cross-border financial tracing and international law-enforcement cooperation**.
- India is not a party to the **Budapest Convention on Cybercrime**; India's approach has historically emphasised a broader international framework that gives greater weight to State sovereignty and participation of developing countries.

Way Forward:

Strengthen the First-Response System:

- Integrate **1930, NCRP, banks, payment systems and police control rooms** into a genuinely real-time response architecture.

Kamaraj IAS Academy

Plot A P.127, AF block, 6 th street, 11th Main Rd, Shanthi Colony, Anna Nagar, Chennai, Tamil Nadu 600040

Phone: **044 4353 9988 / 98403 94477 / Whatsapp : 09710729833**

- Standardise rapid freezing of suspicious accounts and strengthen mechanisms for subsequent grievance resolution and legitimate restoration of funds.

Build Grassroots Cyber-Forensics:

- Expand trained cyber investigators and forensic laboratories beyond specialised metropolitan centres.
- Police stations should have access to trained personnel capable of handling **device seizure, digital imaging, metadata, hash verification, electronic evidence preservation and chain of custody**.

Adopt Risk-Based AI Governance:

- Deepfake regulation should combine **traceability, labelling, platform accountability and rapid removal of unlawful content** with safeguards for legitimate AI innovation and lawful expression.
- Continuous technological updating is essential because generative AI capabilities evolve faster than conventional regulatory cycles.

Strengthen Financial Cybersecurity:

- Banks and payment platforms should deploy stronger **real-time anomaly detection, mule-account identification, transaction-risk scoring and behavioural analytics**.
- Faster information sharing between financial institutions and law-enforcement agencies can reduce the time available to fraudsters for layering and withdrawing funds.

Improve Cyber Awareness:

- Awareness campaigns should move beyond generic warnings and provide **scenario-based training** covering digital arrest scams, investment fraud, phishing, fake delivery calls, impersonation and malicious applications.
- Schools, colleges, senior-citizen networks and workplaces should be integrated into digital-safety programmes.

Value Addition for UPSC:

Prelims Facts:

- **NCRB:** Established in 1986; Ministry of Home Affairs; headquarters in New Delhi.
- **CERT-In:** National nodal agency for cybersecurity incident response; statutory basis under **Section 70B, IT Act**.
- **NCIIPC:** Critical Information Infrastructure protection; statutory basis under **Section 70A, IT Act**.
- **I4C:** Ministry of Home Affairs; coordinates law-enforcement response to cybercrime.
- **NCRP:** National Cyber Crime Reporting Portal.
- **1930:** Helpline for reporting financial cyber fraud.
- **CFCFRMS:** Immediate reporting and coordinated response to financial cyber fraud.
- **Section 66C:** Identity theft.
- **Section 66D:** Cheating by personation using computer resources or communication devices.
- **Section 66F:** Cyber terrorism.
- **Section 69A:** Blocking of public access to specified information.
- **Section 63, BSA:** Electronic-record admissibility framework.
- **Police and Public Order:** State List subjects.