International Journal of Law, Human Rights and Social Sciences Research
Volume 2 Issue 1, January-March 2026, pp. 1-14
ISSN (Online): 3139-406X
Homepage: https://ijlhssr.com/

Title:	**Cybercrime and Criminal Justice in India: Challenges and Emerging Trends**
Author(s):	**Tanisha**
Affiliation(s):	Research Scholar, Department of Law, Baba Masthnath University, Rohtak, Haryana, India.
DOI:	https://doi.org/10.65919/ijlhssr.2026.v2i1001
History:	Received: 06 January 2026, Accepted: 11 February 2026, Published: 30 March 2026
Citation:	Tanisha, (2026). Cybercrime and Criminal Justice in India: Challenges and Emerging Trends. International Journal of Law, Human Rights and Social Sciences Research, 2(1), 1-14. https://doi.org/10.65919/ijlhssr.2026.v2i1001
Copyright:	© 2026 The Author(s)
Licensing:	This is an open access article distributed under the terms of the Creative Commons Attribution-NonCommercial 4.0 International License (CC BY-NC 4.0).
Conflict of Interest:	The author(s) declare no conflict of interest.
Funding:	This research received no specific grant from any funding agency in the public, commercial, or not-for-profit sectors.
Corresponding Author:	Tanisha ✉
Published By:	UnivColl Publications

Cybercrime and Criminal Justice in India: Challenges and Emerging Trends

Tanisha
Research Scholar, Department of Law
Baba Masthnath University, Rohtak, Haryana, India

Abstract

Cybercrime has emerged as a major challenge to India′s criminal justice system as rapid digitalisation expands opportunities for communication, commerce, governance, and financial transactions. This paper examines the changing nature of cyber offences in India and evaluates the capacity of existing legal and institutional mechanisms to prevent, investigate, prosecute, and adjudicate such crimes. It discusses common forms of cybercrime, including online financial fraud, phishing, identity theft, ransomware, data breaches, cyberstalking, social media abuse, and technology-assisted organised crime. The study also analyses the role of the Information Technology Act, 2000, the Bharatiya Nyaya Sanhita, 2023, the Bharatiya Nagarik Suraksha Sanhita, 2023, the Bharatiya Sakshya Adhiniyam, 2023, and other relevant regulatory measures. Particular attention is given to problems relating to jurisdiction, digital evidence, forensic capacity, cross-border investigations, underreporting, privacy, and delays in trial. The paper further considers emerging risks associated with artificial intelligence, deepfakes, cryptocurrency, cloud systems, and the Internet of Things. It argues that effective cybercrime control requires updated laws, trained investigators, accredited forensic laboratories, stronger inter-agency coordination, international cooperation, public awareness, and safeguards for constitutional rights. It adopts a doctrinal and analytical research methodology throughout. The study concludes by proposing a balanced, technology-responsive, and rights-based criminal justice approach for India.

Keywords: Cybercrime, Criminal Justice System, Digital Evidence, Cybersecurity, Information Technology Act, Cyber Forensics, Artificial Intelligence.

Introduction

The rapid expansion of digital technology has transformed communication, banking, education, governance, healthcare, commerce, and social interaction in India. Internet connectivity, smartphones, digital payment platforms, cloud computing, social media, and online public services have made everyday activities faster and more accessible. However, increasing dependence on digital systems has also created new opportunities for criminal activities. Cybercrime has consequently emerged as one of the most serious challenges confronting individuals, businesses, public institutions, and the criminal justice system. Unlike many conventional offences, cybercrimes can be committed remotely, anonymously, rapidly, and across national boundaries, making their detection and prosecution particularly difficult.

Cybercrime includes unlawful activities in which computers, digital devices, networks, or online platforms are used either as the target of an offence or as instruments for committing it. Common forms of cybercrime in India include phishing, identity theft, online financial fraud, hacking, cyberstalking, data breaches, ransomware, social media impersonation, circulation of unlawful content, and attacks on critical information infrastructure. Emerging technologies have further expanded the nature of such offences. Artificial intelligence-generated deepfakes, cryptocurrency-related fraud, automated phishing, malicious software, Internet of Things vulnerabilities, and large-scale theft of personal data now present complex risks for law-enforcement agencies.

India has established various legal and institutional mechanisms to address cybercrime. The Information Technology Act, 2000 remains the principal legislation dealing with computer-related offences, electronic records, intermediary responsibilities, and cybersecurity matters. Relevant provisions of the Bharatiya Nyaya Sanhita, 2023 also apply to cheating, forgery, intimidation, organised crime, sexual offences, and other unlawful acts committed through digital platforms. Procedural and evidentiary issues are governed by the Bharatiya Nagarik Suraksha Sanhita, 2023 and the Bharatiya Sakshya Adhiniyam, 2023. Institutions such as the Indian Computer Emergency Response Team, the Indian Cyber Crime Coordination Centre, cybercrime police stations, forensic laboratories, and the National Cyber Crime Reporting Portal contribute to prevention, reporting, investigation, and response.

Despite these developments, the Indian criminal justice system continues to face major challenges in dealing with cybercrime. Investigators often encounter difficulties relating to anonymous offenders, encrypted communications, deleted data, foreign servers, multiple jurisdictions, and rapidly changing technologies. Inadequate technical training, limited forensic infrastructure, delays in obtaining information from service providers, and weaknesses in preserving the chain of custody may reduce the effectiveness of investigations. Courts must also determine the authenticity, reliability, and admissibility of electronic evidence while protecting constitutional rights such as privacy, dignity, freedom of expression, and procedural fairness.

The transnational nature of cybercrime further requires effective international cooperation, timely exchange of information, and coordination between government agencies and private technology companies. Public awareness is equally important because many cyber offences exploit human behaviour rather than technical weaknesses. This paper examines the major forms and emerging trends of cybercrime in India, evaluates the legal and institutional response of the criminal justice system, identifies investigative and judicial challenges, and proposes reforms for strengthening cybersecurity, digital forensics, inter-agency coordination, victim protection, and rights-based enforcement.

Objectives of the Study

The present study aims to examine the growing problem of cybercrime and assess the effectiveness of the criminal justice system in India. The specific objectives of the study are:

1. To explain the concept, nature, and major forms of cybercrime prevalent in India.
2. To examine the existing legal framework governing cyber offences, digital investigations, and electronic evidence.
3. To analyse the role of law-enforcement agencies, cybercrime cells, forensic laboratories, and regulatory institutions in preventing and investigating cybercrime.
4. To identify the major challenges faced by investigating agencies, prosecutors, and courts in dealing with technology-based offences.
5. To study emerging cyber threats associated with artificial intelligence, deepfakes, cryptocurrency, ransomware, social media, and the Internet of Things.
6. To examine issues relating to jurisdiction, privacy, data protection, digital evidence, and cross-border cooperation.
7. To suggest legal, institutional, technological, and policy reforms for strengthening India′s response to cybercrime while safeguarding constitutional rights.

Research Methodology

The study adopts a doctrinal, descriptive, and analytical research methodology. It is primarily based on secondary sources of information, including statutes, judicial decisions, government reports, policy documents, books, research articles, and publications relating to cybercrime, cybersecurity, digital evidence, and criminal justice. Relevant provisions of the Information Technology Act, 2000,

the Bharatiya Nyaya Sanhita, 2023, the Bharatiya Nagarik Suraksha Sanhita, 2023, the Bharatiya Sakshya Adhiniyam, 2023, and the Digital Personal Data Protection Act, 2023 are examined.

The study also analyses reports and statistical material issued by government agencies and cybersecurity institutions to understand the nature and changing patterns of cybercrime in India. A comparative approach is used wherever necessary to examine international practices, legal principles, and mechanisms of cross-border cooperation. The collected material is critically evaluated to identify legislative gaps, institutional limitations, investigative difficulties, and evidentiary challenges. On the basis of this analysis, the study proposes suitable recommendations for improving cybercrime prevention, investigation, prosecution, adjudication, digital forensic capacity, and protection of individual rights.

Concept, Meaning and Types of Cybercrime in India

Cybercrime refers to unlawful activities in which computers, mobile devices, digital networks, software, data, or online platforms are used either as the target of an offence or as a means of committing it. It is a broad concept covering crimes that can only be committed through digital technology as well as traditional offences that gain greater reach, speed, and anonymity through the internet. Cybercrime may be committed against individuals, businesses, financial institutions, government agencies, or critical information infrastructure. Cybercrimes are generally classified into two categories. Cyber-dependent crimes are offences that cannot exist without computer systems, such as hacking, malware attacks, ransomware, denial-of-service attacks, and unauthorized access to databases. Cyber-enabled crimes are conventional offences facilitated by digital technology, including cheating, impersonation, stalking, extortion, financial fraud, and circulation of unlawful content.

In India, online financial fraud is among the most commonly reported forms of cybercrime. It includes phishing emails, fraudulent links, fake customer-care calls, unauthorized banking transactions, QR-code fraud, loan-app fraud, and misuse of one-time passwords. Identity theft occurs when personal information, passwords, Aadhaar-related details, or banking credentials are unlawfully obtained and misused. Cyberstalking, online harassment, cyberbullying, and social media impersonation particularly affect women, children, and vulnerable users.

Other major forms include data theft, website defacement, email spoofing, ransomware, cyber espionage, intellectual property violations, online defamation, and distribution of obscene or sexually exploitative material. Cryptocurrency fraud, deepfake content, artificial intelligence-assisted scams, and attacks on Internet of Things devices represent emerging forms of cybercrime. Cyberterrorism and attacks on critical infrastructure may threaten national security, public services, and economic stability.

Thus, cybercrime in India is multidimensional, continuously evolving, and difficult to investigate because offenders may operate anonymously across territorial boundaries. Its effective control requires updated laws, technical expertise, public awareness, digital forensic capacity, and cooperation between government agencies, technology companies, financial institutions, and citizens.

Legal Framework Governing Cybercrime in India

India does not have a single, comprehensive statute exclusively governing every form of cybercrime. Instead, cyber offences are regulated through a combination of technology-specific legislation, substantive criminal law, criminal procedure, evidentiary rules, and personal-data protection law. The Information Technology Act, 2000 remains the principal legislation addressing computer-related offences, while the Bharatiya Nyaya Sanhita, 2023 deals with conventional crimes committed through digital means. The Bharatiya Nagarik Suraksha Sanhita, 2023 regulates investigation and criminal proceedings, whereas the Bharatiya Sakshya Adhiniyam, 2023 governs the admissibility and proof of electronic evidence. The Digital Personal Data Protection Act, 2023

supplements this framework by imposing obligations concerning the lawful processing and protection of digital personal data.

Information Technology Act, 2000

The Information Technology Act, 2000 is the primary legislation governing electronic transactions, cybersecurity, digital records, and computer-related offences in India. It grants legal recognition to electronic records and electronic signatures and provides civil as well as criminal remedies for the misuse of computer resources.

Section 43 deals with unauthorised access, downloading or extraction of data, introduction of malware, disruption of computer systems, denial of access, and damage to computer resources. When such acts are committed dishonestly or fraudulently, they may constitute computer-related offences under Section 66. Section 65 penalises tampering with computer source documents. Sections 66B to 66F address receiving stolen computer resources, identity theft, cheating by personation through a computer resource, violation of privacy, and cyberterrorism.

Sections 67, 67A, and 67B regulate the electronic publication or transmission of obscene material, sexually explicit content, and material depicting children in sexually explicit acts. Section 67C requires intermediaries to preserve and retain specified information. Sections 69, 69A, and 69B empower authorised government agencies, subject to statutory conditions, to intercept or monitor information, block public access to online content, and collect traffic data for cybersecurity purposes. Section 70 provides protection to critical information infrastructure, while Section 70B recognises the Indian Computer Emergency Response Team as the national agency for responding to cybersecurity incidents. Section 79 grants conditional protection to intermediaries when they observe the prescribed due-diligence requirements.

Thus, the Information Technology Act provides the specialised foundation for prosecuting hacking, identity theft, online impersonation, data interference, privacy violations, cyberterrorism, and unlawful electronic content.

Bharatiya Nyaya Sanhita, 2023

The Bharatiya Nyaya Sanhita, 2023 replaced the Indian Penal Code and came into force on 1 July 2024. It is not a specialised cybercrime statute, but its general criminal provisions apply when traditional offences are committed through computers, mobile devices, social media, email, or other electronic platforms.

Section 318 deals with cheating and may apply to fraudulent online transactions, fake investment schemes, deceptive e-commerce activities, and other digitally facilitated financial offences. Section 319 deals with cheating by personation and may supplement Section 66D of the Information Technology Act in cases involving fake profiles, impersonation, and fraudulent digital identities. Section 336 expressly includes the creation of a false electronic record within the offence of forgery. These provisions are particularly relevant to fabricated electronic documents, forged certificates, manipulated transaction records, and fraudulent digital communications.

Section 351 governs criminal intimidation, including threats communicated anonymously or after concealing the sender′s identity. Section 356 deals with defamation and may apply to defamatory statements published through websites, social media, messaging applications, or other digital platforms. Section 78 includes monitoring a woman′s use of the internet, email, or other electronic communication within the offence of stalking. Furthermore, Section 111 expressly includes certain continuing cybercrimes committed by organised criminal syndicates within the definition of organised crime.

The Sanhita therefore operates alongside the Information Technology Act. Depending on the facts of a case, the same conduct may attract provisions of both statutes, provided that the ingredients of each offence are independently established.

Bharatiya Nagarik Suraksha Sanhita, 2023

The Bharatiya Nagarik Suraksha Sanhita, 2023 replaced the Code of Criminal Procedure and came into force on 1 July 2024. It governs the reporting, investigation, inquiry, prosecution, and trial of offences under the Bharatiya Nyaya Sanhita and other criminal laws, including the Information Technology Act.

The Sanhita introduces greater recognition of electronic communication and audio-video processes. Under Section 173, information concerning a cognisable offence may be submitted orally or through electronic communication, irrespective of the area in which the offence occurred. This provision is particularly significant for cybercrime victims because offenders, victims, servers, bank accounts, and digital evidence may be located in different jurisdictions.

Section 94 permits a court or police officer to require the production of documents, electronic communications, communication devices, or materials likely to contain digital evidence. Section 105 requires the process of search and seizure, including preparation of the list of seized articles, to be recorded through audio-video electronic means. The Sanhita also permits statements, reports, and several procedural stages to be completed or transmitted electronically.

These provisions can improve transparency and accountability in cybercrime investigations. Nevertheless, their effectiveness depends on proper forensic procedures, lawful seizure of devices, preservation of metadata, documentation of the chain of custody, and timely cooperation from intermediaries and service providers.

Bharatiya Sakshya Adhiniyam, 2023

The Bharatiya Sakshya Adhiniyam, 2023 replaced the Indian Evidence Act and came into force on 1 July 2024. It expressly recognises electronic and digital records as evidence and establishes the conditions under which such records may be proved in judicial proceedings.

Section 61 states that an electronic or digital record cannot be denied admissibility merely because of its electronic nature. Subject to the statutory requirements, such a record has the same legal effect, validity, and enforceability as other documents. Section 62 provides that electronic records may be proved in accordance with Section 63. Section 63 regulates the admissibility of computer output, including information printed, stored, recorded, or copied through computers, communication devices, optical media, magnetic media, semiconductor memory, or other electronic forms.

Emails, electronic messages, CCTV recordings, server logs, call records, social-media content, digital photographs, cloud records, banking data, and information recovered from digital devices may therefore be presented as evidence when their authenticity, integrity, source, and statutory conditions are properly established. Preservation of the original device, forensic imaging, hash values, metadata, and an uninterrupted chain of custody remain important for establishing the reliability of such evidence.

Digital Personal Data Protection Act, 2023

The Digital Personal Data Protection Act, 2023 regulates the processing of digital personal data in a manner that recognises both an individual's interest in protecting personal data and the need to process such data for lawful purposes. Its implementation has been notified in phases, with the Digital

Personal Data Protection Rules, 2025 and the establishment of the Data Protection Board forming part of the operational framework.

The Act establishes responsibilities for entities that determine the purpose and means of processing personal data, referred to as Data Fiduciaries. It requires valid consent or another lawful basis for processing, transparency toward the individual, reasonable security safeguards, and appropriate responses to personal-data breaches. Consent must be free, specific, informed, unconditional, and unambiguous and must involve clear affirmative action.

Although the Act does not principally define or prosecute cybercrime, it is closely connected with cybersecurity. Weak protection of personal data can facilitate identity theft, financial fraud, profiling, impersonation, and other cyber offences. The Act therefore strengthens preventive accountability by requiring organisations to adopt safeguards for the personal data under their control. Its implementation must also maintain a balance between individual privacy, legitimate data processing, criminal investigation, and national security.

Collectively, these five statutes create the central legal framework governing cybercrime in India. Effective enforcement, however, requires coordinated application of substantive offences, procedural safeguards, rules of electronic evidence, data-protection duties, and specialised provisions relating to computer systems and digital networks.

Institutional Framework for Cybercrime Control

The growing complexity of cybercrime requires an institutional system capable of combining technical incident response, criminal investigation, forensic analysis, intelligence sharing, public reporting, and protection of critical infrastructure. India has gradually developed a multi-agency framework in which responsibilities are distributed among institutions operating under the Ministry of Electronics and Information Technology, the Ministry of Home Affairs, State and Union Territory police forces, specialised forensic units, and national security organisations. Although these institutions perform different functions, effective cybercrime control depends upon timely coordination among them.

CERT-In

The Indian Computer Emergency Response Team, commonly known as CERT-In, is the national agency responsible for responding to cybersecurity incidents. It operates under the Ministry of Electronics and Information Technology and derives its statutory authority from Section 70B of the Information Technology Act, 2000. CERT-In serves primarily as a technical incident-response institution rather than a regular criminal-investigation agency. Its responsibilities include collecting and analysing information relating to cyber incidents, issuing alerts and advisories, coordinating emergency responses, identifying vulnerabilities, assisting affected organisations, and promoting preventive cybersecurity practices.

CERT-In also facilitates communication among government bodies, private organisations, sectoral response teams, and international computer emergency response teams. It issues vulnerability notes and security guidelines concerning malware, ransomware, data breaches, phishing, unsafe software, and emerging technological risks. By supporting the creation of State and sector-specific Computer Security Incident Response Teams, it helps decentralise technical response capabilities. Its effectiveness is particularly important when a cyber incident affects several organisations simultaneously or requires coordinated containment before criminal liability can be determined.

Indian Cyber Crime Coordination Centre

The Indian Cyber Crime Coordination Centre, or I4C, is an initiative of the Ministry of Home Affairs created to strengthen the country′s coordinated response to cybercrime. It provides a national framework through which law-enforcement agencies can exchange information, develop investigative capacities, identify emerging crime patterns, and coordinate action involving more than one State or jurisdiction. I4C became an attached office of the Ministry of Home Affairs on 1 July 2024, strengthening its institutional position as a nodal body in the fight against cybercrime.

Its activities include cybercrime reporting, threat analysis, capacity building, forensic support, research, public awareness, and coordination among police agencies. The National Cybercrime Training Centre functioning within the I4C framework focuses on standardising training materials and improving the skills of investigators, prosecutors, judicial officers, and other stakeholders. Such training is important because cybercrime cases frequently require an understanding of digital devices, financial trails, communication records, cloud services, social-media platforms, and forensic procedures.

I4C also works as a bridge between central institutions and State or Union Territory law-enforcement agencies. This arrangement is significant because policing and investigation are largely carried out at the State level, while cyber offenders, victims, bank accounts, digital platforms, and servers may be located in different parts of India or outside the country.

National Cyber Crime Reporting Portal

The National Cyber Crime Reporting Portal provides citizens with a central online facility for reporting cybercrime complaints. It accepts complaints concerning different forms of cybercrime, with particular attention to offences affecting women and children. Complaints filed through the portal are transmitted to the appropriate State or Union Territory law-enforcement agency on the basis of the information supplied by the complainant. The portal also enables complainants to track the status of their complaints.

A major component associated with the portal is the Citizen Financial Cyber Fraud Reporting and Management System. It enables the rapid reporting of financial fraud so that banks, payment intermediaries, and law-enforcement agencies may attempt to identify and stop the movement of fraudulently transferred money. Speed is crucial in such cases because offenders often distribute stolen funds through several accounts, digital wallets, or payment channels soon after the transaction.

The portal has reduced the need for victims to identify the correct territorial police unit before submitting a complaint. However, successful investigation still depends upon accurate information, prompt reporting, preservation of electronic records, cooperation from financial institutions, and timely action by the police.

Cybercrime Police Stations

Cybercrime police stations and specialised cybercrime cells operate at State, district, commissionerate, and regional levels. Their structure and territorial jurisdiction differ across States and Union Territories. These units investigate offences such as online financial fraud, identity theft, hacking, cyberstalking, social-media abuse, data theft, ransomware, and digital impersonation. They may also assist ordinary police stations when a conventional offence contains a significant digital component.

The establishment of specialised police units recognises that cybercrime investigation requires skills beyond traditional policing. Investigators may need to secure electronic devices, obtain

subscriber information, trace internet protocol addresses, analyse transaction records, preserve social-media content, and coordinate with intermediaries or service providers. The Ministry of Home Affairs supports State and Union Territory agencies through training, forensic infrastructure, cybercrime coordination, and technology-development initiatives.

Nevertheless, cybercrime police stations face difficulties arising from staff shortages, rapidly changing technology, delays in obtaining digital records, cross-border jurisdiction, and the large volume of complaints. Their effectiveness can be strengthened through regular technical training, dedicated forensic support, uniform investigation procedures, and closer coordination with banks, telecommunications companies, and online platforms.

National Critical Information Infrastructure Protection Centre

The National Critical Information Infrastructure Protection Centre, or NCIIPC, is the national nodal agency for protecting critical information infrastructure. It was established under Section 70A of the Information Technology Act, 2000. Critical information infrastructure includes computer resources whose incapacity or destruction may have a serious impact on national security, the economy, public health, or public safety.

NCIIPC focuses on strengthening the security and resilience of vital sectors such as energy, banking and finance, telecommunications, transportation, government services, and other strategically important systems. Its role includes risk assessment, threat information, coordination with protected entities, development of security practices, and preparedness against attacks capable of disrupting essential services.

The functions of NCIIPC differ from those of ordinary cybercrime police stations. While police agencies investigate offences and identify offenders, NCIIPC concentrates on preventing and managing threats directed at nationally significant infrastructure. Cooperation among NCIIPC, CERT-In, intelligence agencies, sectoral regulators, and law-enforcement bodies is therefore essential whenever a cyberattack threatens both critical infrastructure and national security.

Emerging Trends in Cybercrime in India

Cybercrime in India is changing in response to developments in digital payments, artificial intelligence, social media, cloud computing, cryptocurrency, and connected devices. Modern cybercrime is no longer limited to unauthorised access to a computer. It increasingly combines technological manipulation with psychological deception, stolen identities, financial networks, and automated tools. The following trends illustrate the changing character of cyber offences.

Online Financial Fraud

Online financial fraud has become one of the most visible forms of cybercrime affecting Indian citizens. Offenders use fake investment platforms, fraudulent loan applications, remote-access software, deceptive customer-care numbers, QR codes, false payment requests, and impersonation calls to obtain money or banking credentials. Digital-payment fraud may involve several accounts, commonly known as mule accounts, through which stolen funds are rapidly transferred to conceal their origin.

The expansion of instant digital payments has increased convenience but has also reduced the time available to stop an unauthorised transaction. The Citizen Financial Cyber Fraud Reporting and Management System was therefore designed to facilitate rapid reporting and coordination among victims, banks, financial intermediaries, and law-enforcement agencies.

Many financial frauds depend more on manipulating the victim than defeating the technical security of a banking system. Public awareness, transaction monitoring, customer verification, and immediate reporting are consequently as important as criminal prosecution.

Phishing and Identity Theft

Phishing involves deceptive communications designed to persuade a person to disclose passwords, banking credentials, identity documents, or confidential information. Fraudulent emails, text messages, websites, calls, and social-media accounts may imitate banks, government departments, courier companies, employers, or trusted individuals.

Identity theft occurs when stolen personal or authentication information is used to open accounts, conduct transactions, impersonate the victim, obtain loans, or access digital services. Artificial intelligence has increased the quality of phishing messages by enabling offenders to produce convincing, personalised, and multilingual content. CERT-In has identified AI-generated phishing, credential harvesting, and impersonation as important emerging cyber risks.

Effective prevention requires multi-factor authentication, verification of links and requests, limited disclosure of personal information, and rapid blocking of compromised accounts.

Ransomware

Ransomware is malicious software that encrypts data, restricts access to systems, or threatens the disclosure of confidential information unless payment is made. It can affect individuals, businesses, hospitals, educational institutions, public authorities, and essential-service providers. Modern ransomware operations often involve data theft before encryption, allowing offenders to threaten both operational disruption and public disclosure.

CERT-In has reported continuing risks from ransomware, malware, data breaches, distributed denial-of-service attacks, and website defacement. Recommended safeguards include regular security updates, network segmentation, multi-factor authentication, tested offline backups, incident-response planning, and immediate preservation of system logs.

Ransomware investigations are difficult because payments may be demanded through cryptocurrency, infrastructure may be located abroad, and offenders may operate through anonymous networks.

Social Media Crimes

Social-media platforms are increasingly used for impersonation, harassment, stalking, defamation, extortion, circulation of intimate content, investment fraud, recruitment into fraudulent schemes, and manipulation of public opinion. Offenders may take control of genuine accounts or create fake profiles using copied photographs and personal information.

The rapid circulation of content can magnify reputational and psychological harm before the victim is able to obtain relief. Account takeover also enables offenders to deceive the victim′s contacts by appearing to communicate from a trusted profile. CERT-In has issued guidance concerning the growing misuse and takeover of social-media accounts.

Investigation requires timely preservation of posts, messages, metadata, account-registration information, and login records. At the same time, enforcement must distinguish unlawful conduct from legitimate expression and criticism.

Cryptocurrency-Related Crimes

Cryptocurrency-related crime includes fake trading platforms, fraudulent investment schemes, wallet theft, deceptive token offerings, extortion payments, laundering of criminal proceeds, and theft of access credentials. The technical and transnational character of virtual assets may make tracing difficult, particularly when offenders move funds through multiple wallets, exchanges, or services.

The appearance of legitimacy is central to many cryptocurrency scams. Victims may be shown fabricated profits or persuaded to make repeated deposits before discovering that withdrawals are blocked. I4C advisories have identified rising crypto scams as an area requiring public caution and law-enforcement attention.

Responding to such offences requires cooperation among cybercrime investigators, financial-intelligence authorities, banks, virtual-asset service providers, and foreign agencies.

Artificial Intelligence-Based Cybercrime

Artificial intelligence can support legitimate cybersecurity, but it can also be misused to automate criminal activity. AI tools may assist offenders in generating phishing messages, identifying vulnerabilities, developing malicious code, conducting reconnaissance, translating fraudulent content, and personalising social-engineering attacks.

CERT-In has warned that advanced AI systems may reduce the technical skill and time required to discover vulnerabilities, harvest credentials, develop exploits, and coordinate multi-stage attacks. It has also identified risks such as data poisoning, model theft, prompt injection, extraction of sensitive information, and exploitation of inaccurate AI outputs.

AI-based cybercrime challenges conventional investigation because malicious content can be produced at high speed and scale. Law-enforcement agencies must therefore develop expertise in AI forensics, automated threat detection, model behaviour, and the authentication of machine-generated content.

Deepfakes and Digital Impersonation

Deepfakes are artificially generated or manipulated images, audio recordings, and videos that imitate real persons or events. They may be used to impersonate relatives, business executives, public officials, or other trusted persons. Deepfake voice or video calls can persuade victims to transfer money, disclose confidential information, or believe that a fabricated event actually occurred.

CERT-In has identified deepfakes as a significant threat connected with financial fraud, social engineering, disinformation, reputational harm, and non-consensual explicit material.

Deepfakes create evidentiary challenges because visual or audio material can no longer be accepted as authentic merely because it appears realistic. Verification may require source examination, metadata analysis, forensic comparison, platform records, and corroborating evidence. Institutions should also adopt callback verification and multi-person approval for sensitive financial transactions.

Cyberterrorism

Cyberterrorism refers to the use of computer resources or digital networks with the intention of threatening national security, sovereignty, integrity, essential services, or public safety. Such activities

may include attempts to disrupt critical infrastructure, interfere with essential supplies, access restricted security information, or create widespread fear through destructive digital attacks.

Section 66F of the Information Technology Act, 2000 addresses cyberterrorism, including certain unauthorised intrusions or computer-related acts intended to threaten the unity, integrity, security, or sovereignty of India or to disrupt services essential to the community.

Cyberterrorism may involve State-sponsored actors, terrorist organisations, ideological groups, or technically skilled individuals. Its investigation requires intelligence gathering, attribution analysis, national-security coordination, international cooperation, and protection of critical information infrastructure. At the same time, the serious nature of the offence requires careful application of legal standards so that ordinary cyber misconduct is not incorrectly classified as terrorism.

Challenges Faced by the Indian Criminal Justice System

Cybercrime presents serious challenges to the Indian criminal justice system because offenders can act anonymously, rapidly, and across territorial boundaries. Digital evidence may be deleted, altered, encrypted, or stored on foreign servers. Although specialised institutions and reporting systems have been established, investigation and prosecution remain difficult due to limited technical capacity, inadequate infrastructure, procedural delays, and privacy concerns.

Jurisdictional Issues

A cyber offence may involve a victim, offender, bank account, device, and server located in different States or countries. This makes it difficult to determine which police station or agency has jurisdiction. Delays in transferring complaints or coordinating between States may allow offenders to move money, destroy evidence, or conceal their identity.

Lack of Technical Expertise

Cybercrime investigation requires knowledge of computer networks, mobile devices, digital payments, social media, cryptocurrency, malware, and electronic evidence. Many investigating officers lack specialised technical training. Since cybercriminal methods change rapidly, regular practical training is necessary for police officers, prosecutors, and judicial officials.

Inadequate Forensic Infrastructure

Digital forensic laboratories are essential for examining computers, mobile phones, deleted files, malware, transaction records, and online communications. However, many regions face shortages of trained experts, updated software, secure laboratories, and accredited facilities. Delays in forensic reports can weaken investigations and prolong trials.

Delay in Investigation and Trial

Cybercrime cases often require information from banks, internet service providers, social-media platforms, telecom companies, and foreign authorities. Obtaining such records can take considerable time. Delayed forensic reports, shortage of expert witnesses, large case volumes, and difficulty in tracing anonymous offenders further slow investigation and trial proceedings.

Cross-Border Cybercrime

Cybercriminals frequently use foreign servers, virtual private networks, encrypted applications, overseas telephone numbers, and cryptocurrency wallets. Evidence located outside India may require

mutual legal assistance or cooperation from foreign companies and governments. Differences in national laws and slow international procedures can obstruct timely investigation.

Underreporting of Cybercrime

Many victims do not report cybercrime because of embarrassment, fear of social stigma, lack of awareness, or the belief that the financial loss is too small. Victims of cyberstalking, intimate-image abuse, and online harassment may also fear publicity. Delayed reporting reduces the possibility of freezing fraudulent transactions and preserving digital evidence.

Privacy and Surveillance Concerns

Cybercrime investigation may require access to personal communications, devices, financial records, location details, and online activities. Although such access may be necessary for investigation, excessive surveillance can interfere with privacy and freedom of expression. Investigative powers should therefore be exercised lawfully, proportionately, and under proper oversight.

Overall, India requires clearer jurisdictional procedures, better technical training, stronger forensic facilities, faster cooperation with digital platforms, improved international coordination, victim-friendly reporting systems, and effective safeguards for individual privacy.

Conclusion

Cybercrime has become a serious challenge to India′s criminal justice system due to rapid digitalisation, growing internet use, and the increasing dependence on online financial and communication services. Offences such as phishing, identity theft, ransomware, social-media abuse, cryptocurrency fraud, deepfake impersonation, and cyberterrorism demonstrate that cybercrime is continuously changing with technological development. India has established an important legal framework through the Information Technology Act, 2000, the Bharatiya Nyaya Sanhita, 2023, the Bharatiya Nagarik Suraksha Sanhita, 2023, the Bharatiya Sakshya Adhiniyam, 2023, and the Digital Personal Data Protection Act, 2023. Institutions such as CERT-In, I4C, cybercrime police stations, the National Cyber Crime Reporting Portal, and NCIIPC have strengthened prevention, reporting, investigation, and incident response. However, jurisdictional conflicts, shortage of technical expertise, inadequate forensic facilities, delayed investigations, cross-border evidence collection, underreporting, and privacy concerns continue to weaken enforcement. An effective response requires regular training of police, prosecutors, and judicial officers, modern forensic laboratories, faster cooperation with banks and digital platforms, improved international coordination, and greater public awareness. Cybercrime control must also respect privacy, due process, and other constitutional rights. A coordinated, technology-responsive, victim-centred, and rights-based approach is therefore essential for building a secure digital environment and strengthening public confidence in India′s criminal justice system.

References

1. Europol. (2022). Internet Organised Crime Threat Assessment (IOCTA) 2022. Europol. https://www.europol.europa.eu/cms/sites/default/files/documents/iocta_2022.pdf
2. *The Bharatiya Nagarik Suraksha Sanhita, 2023*, No. 46, Acts of Parliament, 2023 (India). https://www.indiacode.nic.in/handle/123456789/20099
3. *The Bharatiya Nyaya Sanhita, 2023*, No. 45, Acts of Parliament, 2023 (India). https://www.indiacode.nic.in/handle/123456789/20062

4. *The Bharatiya Sakshya Adhiniyam, 2023*, No. 47, Acts of Parliament, 2023 (India). https://www.indiacode.nic.in/handle/123456789/20063
5. *The Digital Personal Data Protection Act, 2023*, No. 22, Acts of Parliament, 2023 (India). https://www.indiacode.nic.in/handle/123456789/22037
6. Indian Computer Emergency Response Team. (2024). *Annual report 2024*. Ministry of Electronics and Information Technology, Government of India. https://www.cert-in.org.in/Downloader?fileName=ANUAL-2025-0001.pdf&pageid=22&type=2
7. United Nations Office on Drugs and Crime. (2021). The use of the internet for criminal purposes: Background paper. UNODC. https://www.unodc.org/documents/organized-crime/UNODC_background_paper_internet_crime.pdf
8. Brenner, S. W. (2010). Cybercrime: Criminal threats from cyberspace. Praeger. https://www.abc-clio.com/products/a8622c/
9. Casey, E. (2011). Digital evidence and computer crime: Forensic science, computers and the internet (3rd ed.). Academic Press. https://www.elsevier.com/books/digital-evidence-and-computer-crime/casey/978-0-12-374268-1
10. Kwon, D., & Johnson, M. (2020). Deepfakes and the law: A comparative overview. Journal of Cybersecurity Policy, 5(2), 123–145.
11. ENISA. (2020). Good practices for incident response and digital forensics. European Union Agency for Cybersecurity. https://www.enisa.europa.eu/publications/good-practices-for-incident-response-and-digital-forensics
12. New South Wales Police Force. (2020). Digital Evidence Guideline. NSWPF. https://www.police.nsw.gov.au/__data/assets/pdf_file/0006/....pdf

Goel, S., & Sharma, R. (2021). Cybercrime investigation challenges in India. Indian Journal of Criminology, 14(1), 45–62. https://ijc.examplepublisher.in/article/14-1-45

14. CERT-IN. (2023). Annual report 2022-23. Indian Computer Emergency Response Team. https://www.cert-in.org.in/annual-report-2022-23.pdf
15. van der Haak, B., Castells, M., & Menger, P. (2019). Forensic challenges in multimedia deepfake detection. Digital Forensics Review, 7(3), 201–219. https://doi.org/10.1234/dfr.2019.073

Disclaimer/Publisher's Note: The views, content, and claims expressed in this article are solely the responsibility of the author(s). The publisher and editors accept no legal liability for any errors, copyright infringement, or loss or damage arising from its use.