The Indian Journal for Research in Law and Management

Open Access Law Journal – Copyright © 2026

Editor-in-Chief – Dr. Muktai Deb Chavan; Publisher – Alden Vas; ISSN: 2583-9896

COMBATING CYBER-CRIMES IN INDIA: AN ANALYSIS OF EMERGING THREATS AND LEGAL RESPONSES

~Arunendra Kumar Sharma

ABSTRACT:

The rapid growth of digital technology and internet accessibility has transformed communication, commerce and governance in India. However, this technological advancement has simultaneously led to a significant rise in cyber-crimes such as ***phishing, identity theft, ransomware attacks, cyber stalking, financial fraud and data breaches****. The emergence of artificial intelligence, deepfake technology and cryptocurrency-based transactions has further complicated the nature of cyber offences and created new challenges for law enforcement agencies. This research paper examines the evolving nature of cyber-crimes in India and critically analyses the adequacy of existing legal responses. It studies the provisions of the* ***Information Technology Act, 2000, the Bharatiya Nyaya Sanhita, 2023 and the Digital Personal Data Protection Act, 2023*** *in addressing contemporary cyber threats. The paper further explores the challenges associated with investigation, jurisdiction, digital evidence and cross border cyber offences.*

The paper argues that although India has developed an expanding legal framework to combat cyber-crimes, rapid technological advancement continues to outpace legislative and institutional preparedness. The study concludes that India's cyber law regime must continuously evolve in order to balance technological innovation, national security and protection of constitutional liberties in the digital era.

KEYWORDS: Cyber Crime, Artificial Intelligence, Cyber Security, Data Protection, Information Technology Act, Digital Evidence, Online Fraud.

INTRODUCTION

The rapid expansion of digital technology has fundamentally transformed modern society. In recent years, India has witnessed unprecedented growth in internet accessibility, digital banking, online communication and technology driven governance. Government initiatives such as **Digital India,** increasing smartphone penetration and the expansion of e-commerce platforms have significantly accelerated the country's digital transformation. While these developments have improved connectivity, convenience and economic growth, they have simultaneously exposed individuals, institutions and governments to increasing cyber security threats. In the contemporary digital era, crimes are no longer confined to physical spaces; they are increasingly committed through computers, online networks and digital platforms operating across national boundaries.

Cyber-crimes have emerged as one of the most serious challenges confronting modern legal systems. Offences such as phishing, identity theft, ransomware attacks, online financial fraud, cyber stalking, data breaches and hacking have increased rapidly in both frequency and complexity. The emergence of **artificial intelligence, cryptocurrency transactions, deepfake technology and anonymous digital networks has further transformed the nature of cyber offences.** Unlike traditional crimes, Cyber-crimes are often borderless, technologically sophisticated and difficult to investigate due to issues relating to anonymity, encryption and jurisdiction. These offences not only threaten financial security and individual privacy, but also endanger national security, public order and the integrity of digital governance systems.[1]

India, being one of the fastest growing digital economies in the world, has become increasingly vulnerable to cyber-attacks and digital exploitation. According to recent reports published by the **National Crime Records Bureau,** cyber related offences have shown a substantial increase over the past decade. The growing dependence upon digital infrastructure after the **COVID-19 pandemic** has further intensified concerns regarding online fraud, misuse of personal data and cyber enabled financial crimes. At the same time, technological advancement has frequently outpaced legislative and institutional preparedness, thereby creating significant gaps in cyber regulation and enforcement mechanisms.[2]

This research paper critically examines the **emerging forms of Cyber-crimes in India** and analyses the effectiveness of existing legal responses. It further explores the challenges faced

[1] R. K. Chaubey, Emerging Challenges of Cyber Crimes in India, 8 Int'l J. Legal Stud. 112 (2022).
[2] National Crime Records Bureau, https://www.ncrb.gov.in (last visited May 28, 2026).

by investigative agencies, the role of judicial interpretation and the need for stronger regulatory and institutional mechanisms in order to combat Cyber-crimes in the digital age.

LITERATURE REVIEW

1. **Maria Bada & Jason R. C. Nurse, "Profiling the Cybercriminal: A Systematic Review of Research" (2021) -** The authors conducted a systematic review of cybercrime research and examined the behavioural patterns, motivations, and characteristics of cybercriminals. The study highlights the absence of a universally accepted framework for profiling cyber offenders and emphasizes the need for interdisciplinary approaches involving law enforcement, criminology, and cybersecurity. It concludes that understanding offender behaviour is essential for developing effective cybercrime prevention and response mechanisms.[3]

Research Gap:

While the study provides a comprehensive analysis of cybercriminal profiling, it does not examine the adequacy of India's legal framework in addressing emerging cyber threats. The constitutional and statutory responses to cybercrime in India remain insufficiently explored.

2. **Lavanya Elluri et al., "Recent Advancements in Machine Learning for Cybercrime Prediction" (2023) -** This study reviews recent developments in machine learning techniques for predicting and detecting cybercrime. It discusses anomaly detection, deep learning, transfer learning, and reinforcement learning models that enhance cyber threat prediction. The authors also identify emerging datasets and future research directions for proactive cyber defence.[4]

Research Gap:

Although the paper extensively discusses technological advancements, it gives limited attention to the legal and regulatory framework governing the use of such technologies in India, particularly under the Information Technology Act and related laws.

3. **Mariam Nouh, Jason R. C. Nurse, Helena Webb & Michael Goldsmith, "Cybercrime Investigators are Users Too! Understanding the Socio-Technical**

[3] Maria Bada & Jason R. C. Nurse, Profiling the Cybercriminal: A Systematic Review of Research (2021), https://arxiv.org/abs/2105.02930 (last visited May 28, 2026).
[4] Lavanya Elluri et al., Recent Advancements in Machine Learning for Cybercrime Prediction (2023), https://arxiv.org/abs/2304.04819 (last visited May 28, 2026).

Challenges Faced by Law Enforcement" (2019) - The authors examine the practical and technical challenges encountered by cybercrime investigators through interviews with law enforcement professionals. The study identifies issues such as lack of technological resources, inadequate training, and difficulties in digital investigations, emphasizing the need for improved investigative support systems.[5]

Research Gap:

The study focuses primarily on operational challenges faced by investigators but does not analyse how India's legal framework can be strengthened to improve cybercrime investigation and prosecution.

4. **N. S. Nappinai, "Cyber Crime Law in India: Has Law Kept Pace with Emerging Trends? An Empirical Study" (2010) -** The author critically evaluates India's cyber law regime and examines whether existing legislation adequately addresses evolving forms of cybercrime. The study identifies legislative gaps relating to investigation, enforcement, and technological developments, while advocating continuous legal reforms to address emerging cyber threats.[6]

Research Gap:

The study predates recent developments such as AI-enabled cybercrime, ransomware attacks, deepfake technology, and the Digital Personal Data Protection Act, 2023. Consequently, there remains a need to evaluate whether India's contemporary legal framework is capable of addressing these emerging cyber threats.

RESEARCH METHODOLOGY

The present study adopts a **doctrinal and analytical** method of research to examine the growing challenge of cybercrimes in India and the effectiveness of the existing legal framework. The study is based on both **primary** and **secondary** sources. Primary sources include the Constitution of India, the Information Technology Act, 2000, the Bharatiya Nyaya Sanhita, 2023, the Digital Personal Data Protection Act, 2023, and relevant judicial decisions.

[5] Mariam Nouh, Jason R. C. Nurse, Helena Webb & Michael Goldsmith, Cybercrime Investigators are Users Too! Understanding the Socio-Technical Challenges Faced by Law Enforcement (2019), https://arxiv.org/abs/1902.06961 (last visited May 28, 2026).
[6] N. S. Nappinai, Cyber Crime Law in India: Has Law Kept Pace with Emerging Trends? An Empirical Study, https://www.jiclt.com/index.php/jiclt/article/view/52 (last visited May 28, 2026).

Secondary sources include books, journal articles, research papers, government reports, and other credible academic publications.

The study further adopts an analytical approach to evaluate emerging cyber threats, identify challenges in the existing legal framework, and suggest reforms for strengthening cybercrime regulation in India.

UNDERSTANDING CYBER-CRIMES

I. Meaning and Nature of Cyber-crimes:

The term **cyber-crime** refers to unlawful activities committed through computers, digital devices, online networks or internet-based platforms. In simple terms, cyber-crimes are offences where a computer, digital technology or network either becomes the target of the crime or is used as a tool for committing the offence. Unlike traditional crimes which generally occur within a physical environment, cyber-crimes are committed within the digital sphere and are often capable of affecting victims across multiple jurisdictions simultaneously.[7]

One of the most distinctive characteristics of cyber-crimes is their **borderless and anonymous nature**. Cyber offenders can operate remotely from different countries while concealing their identity through encryption technologies, fake IP addresses and anonymous networks. This creates serious challenges for law enforcement agencies in identifying offenders and establishing jurisdiction. In many cases, cyber-attacks are executed within seconds and may result in substantial financial losses, reputational harm and unauthorized disclosure of sensitive personal information.[8]

In the contemporary digital society, cyber-crimes are no longer limited to individual victims alone. Large corporations, financial institutions, government agencies and even critical national infrastructure have increasingly become targets of cyber-attacks. As a result, cyber-crime today represents not merely a technological issue, but also a significant legal, economic and national security concern requiring continuous legal and institutional adaptation.

II. Characteristics of Cyber-crimes:

Cyber-crimes possess several unique characteristics that distinguish them from conventional offences. The rapidly evolving nature of technology has made cyber offences more

[7] Vakul Sharma, Information Technology Law and Practice (Universal Law Publishing 2011).
[8] Aparna Viswanathan, Cyber Law: Indian and International Perspectives on Key Topics Including Data Security, E-Commerce and Cloud Computing (LexisNexis 2012).

sophisticated, difficult to trace and capable of affecting a large number of victims simultaneously. Understanding these characteristics is essential for developing effective legal and investigative responses.[9]

1. **Borderless Nature**

One of the most significant features of cyber-crimes is their **transnational character**. Cyber offenders can commit offences from any part of the world without physically entering the territory where the harm occurs. This often creates complex jurisdictional issues and difficulties in international investigation and prosecution.

2. **Anonymity of Offenders**

Cyber criminals frequently conceal their identity through **fake IP addresses, encrypted networks, VPN services and anonymous digital platforms**. This anonymity makes identification and trace of the offenders extremely difficult for law enforcement agencies.

3. **Technological Sophistication**

Modern cyber offences involve advanced technologies such as **artificial intelligence, malware, ransomware, deepfake software and automated hacking tools**. As technology evolves, cyber-crimes continue to become more complex and technically challenging.

4. **Speed and Large-Scale Impact**

Unlike traditional offences, cyber-attacks can be executed within seconds and may affect millions of individuals or institutions simultaneously. A single data breach or ransomware attack may result in enormous financial losses and compromise sensitive information on a massive scale.

5. **Dependence on Digital Evidence**

Cyber-crimes primarily involve **electronic records, server logs, metadata, emails, IP addresses and digital transactions** rather than physical evidence. Preservation and admissibility of such evidence often become major challenges during investigation and trial.

6. **Rapidly Evolving Nature**

Cyber-crime techniques constantly evolve alongside technological development. New forms

[9] R. K. Chaubey, Emerging Challenges of Cyber Crimes in India, 8 Int'l J. Legal Stud. 112 (2022).

of offences such as **AI generated frauds, deepfake impersonation and crypto related crimes** continue to emerge faster than legislative and regulatory mechanisms can adapt.

7. Threat to National Security and Public Order

Cyber-attacks are no longer limited to individual victims. Government databases, banking systems, defence networks and critical infrastructure have increasingly become targets of cyber terrorism and digital warfare, making cyber security an issue of national importance.

III. Cyber-crimes and Traditional Crimes:

Although both Cyber-crimes and traditional crimes involve unlawful conduct, the nature, method and impact of cyber offences differ significantly from conventional criminal activities. Technological advancement has transformed the manner in which crimes are planned, executed and investigated, thereby creating new legal and enforcement challenges.[10]

a) Difference in Mode of Commission

Traditional crimes generally involve **physical acts committed within a specific geographical location**, whereas Cyber-crimes are committed through computers, digital devices and online networks. Cyber offenders can operate remotely without any physical presence at the place where harm occurs.

b) Nature of Evidence

Conventional crimes primarily rely upon **physical evidence such as weapons, fingerprints and eyewitness testimony**. In contrast, Cyber-crimes involve electronic evidence including emails, IP addresses, server logs, metadata and digital transaction records. Preservation and authentication of such evidence often require specialized cyber forensic expertise.

c) Jurisdictional Complexity

Traditional offences are usually investigated within a clearly identifiable territorial jurisdiction. However, Cyber-crimes frequently cross-national boundaries and may involve multiple countries simultaneously, making investigation and prosecution significantly more complicated.

d) Anonymity and Identification

[10] Vakul Sharma, Information Technology Law and Practice (Universal Law Publishing 2011).

In traditional crimes, offenders are often physically identifiable. Cyber criminals, on the other hand, can conceal their identity through **encrypted communication, fake accounts, VPN services and anonymous networks**, thereby reducing the risk of detection.

e) Scale and Speed of Harm

Traditional offences generally affect a limited number of victims at a particular time. Cyber-crimes can cause large scale harm within seconds. A single ransomware attack or data breach may compromise sensitive information belonging to millions of individuals simultaneously.

f) Economic and Social Impact

Cyber-crimes frequently target **banking systems, e-commerce platforms, government databases and critical infrastructure**, thereby causing substantial financial losses and threatening public confidence in digital systems. Their impact therefore extends beyond individual victims and may affect the broader economy and national security.

g) Need for Specialized Investigation

Investigation of Cyber-crimes requires technical knowledge relating to **digital forensics, cyber security, encryption technologies and electronic evidence management**. This makes cyber -crime investigation more technologically demanding than investigation of conventional offences.

EMERGING CYBER THREATS IN INDIA

1. Phishing and Financial Fraud:

Among the various forms of Cyber-crimes, **phishing and online financial fraud** have emerged as some of the most widespread and dangerous threats in India. With the rapid growth of digital banking, online payment systems and mobile based financial transactions, cyber criminals have increasingly targeted individuals and financial institutions through deceptive online practices.[11] These offences not only cause significant monetary loss, but also undermine public confidence in digital financial systems.

Phishing refers to a fraudulent technique through which cyber offenders deceive individuals into revealing sensitive personal information such as bank account details, passwords, OTPs, debit card credentials and login information. Such frauds are commonly committed through

[11] Karnika Seth, Computers, Internet and New Technology Laws (LexisNexis 2013).

fake emails, SMS messages, cloned websites, social media links and fraudulent mobile applications designed to imitate legitimate institutions. Victims are often manipulated into believing that the communication originates from trusted entities such as banks, government agencies or e-commerce platforms.

In recent years, India has witnessed a sharp increase in **UPI frauds, OTP scams, QR code frauds and fake customer care scams**. Cyber criminals frequently exploit the lack of digital awareness among users and use psychological manipulation techniques to obtain confidential financial information. The growing use of instant payment platforms and online banking services has further expanded opportunities for financial cyber fraud.[12]

The legal framework governing phishing and financial fraud in India primarily includes provisions under the **Information Technology Act, 2000** and the **Bharatiya Nyaya Sanhita, 2023** relating to cheating, identity theft, personation and unauthorized access to computer systems. Despite these legal provisions, effective enforcement remains challenging due to low reporting rates, technological complexity and the transnational nature of cyber financial crimes.

2. Identity Theft and Data Breaches:

The rapid growth of digital platforms and online services has significantly increased incidents of **identity theft and data breaches** in India. In the contemporary digital economy, personal information such as Aadhaar numbers, bank account details, mobile numbers, passwords and biometric data has become highly valuable. Cyber criminals frequently target such information for financial fraud, impersonation and unauthorized digital activities.

Identity theft occurs when an individual's personal information is stolen and used without authorization for fraudulent purposes. Cyber offenders often misuse stolen identities to open fake bank accounts, obtain loans, conduct online transactions or commit financial fraud in the name of another person. Such offences not only cause financial loss, but also damage the reputation and privacy of victims.

One of the major reasons behind the rise of identity theft is the increasing occurrence of **large-scale data breaches**. Data breaches take place when confidential personal or institutional information is accessed, leaked or stolen without authorization. In recent years, several Indian companies, educational institutions and online platforms have reported incidents involving

[12] Anubha Gupta, Cyber Crimes and Need for Strong Cyber Security Laws in India, 12 Indian J.L. & Tech. 45 (2021).

unauthorized disclosure of sensitive user data. These breaches expose millions of individuals to risks such as fraud, blackmail and cyber exploitation.

Cyber criminals frequently obtain personal information through **phishing attacks, malware infections, hacking, fake mobile applications and unauthorized database access**. The widespread use of cloud storage systems and interconnected digital networks has further increased vulnerability to cyber intrusions. In many cases, leaked personal information is later sold on dark web marketplaces and used for organized cyber-criminal activities.[13]

3. AI Generated Fraud and Deepfake Technology:

Deepfake technology refers to the use of artificial intelligence to create highly realistic but fabricated audio, video or image content. Through deepfake software, cyber offenders can artificially generate a person's voice, facial expressions or appearance in a manner that closely resembles reality. Such manipulated content is often difficult to detect and may be used for fraud, misinformation, defamation, extortion and political manipulation.

In recent years, cyber criminals have increasingly used **AI generated voice cloning and video impersonation** to commit financial frauds. Fraudsters impersonate company executives, bank officials or even family members in order to deceive victims into transferring money or disclosing confidential information. The realistic nature of deepfake content significantly increases the possibility of manipulation and reduces the ability of victims to identify fraudulent communication.

Another serious concern associated with deepfake technology is the spread of **misinformation and digital disinformation**. Manipulated videos and AI generated content may be used to damage reputations, influence elections, spread communal hatred or create public panic. Such misuse poses a serious threat not only to individual privacy and dignity, but also to democratic institutions and public trust in digital information.[14]

4. Ransomware Attacks:

Among modern cyber threats, **ransomware attacks** have emerged as one of the most dangerous and financially damaging forms of cyber-crime. Ransomware is a type of malicious software designed to block access to computer systems, digital networks or sensitive data until a ransom amount is paid to the attackers. These attacks often target businesses, hospitals,

[13] S. K. Verma, Artificial Intelligence and Cyber Security Challenges in India, 15 J. Digital L. & Pol'y 67 (2023).
[14] Talwant Singh, Cyber Law and Information Technology (Allahabad Law Agency 2021).

financial institutions, government agencies and critical infrastructure, causing severe operational disruption and economic loss.

In a typical ransomware attack, cyber criminals gain unauthorized access to a computer system through **malicious email attachments, phishing links, infected software or network vulnerabilities**. Once the malware enters the system, it encrypts files and prevents legitimate users from accessing their own data. The attackers then demand payment, usually in cryptocurrency, in exchange for restoring access to the compromised information.

One of the most serious concerns relating to ransomware attacks is their connection with **organized cyber-criminal networks and international hacking groups**. Many ransomware operations are executed through sophisticated transnational syndicates that operate across multiple jurisdictions. The use of cryptocurrency transactions and anonymous digital networks further complicates tracing and prosecution of offenders.

The emergence of **Ransomware-as-a-Service (RaaS)** has also transformed the cyber-crime landscape. Under this model, skilled cyber criminals develop ransomware software and provide it to other offenders in exchange for a share of the profits. This has increased accessibility of ransomware tools and enabled even less technically skilled individuals to participate in cyber-criminal activities.[15]

5. Cyber Stalking and Online Harassment:

The increasing use of social media platforms, instant messaging applications and digital communication technologies has led to a significant rise in **cyber stalking and online harassment** in India. While digital platforms have improved communication and connectivity, they have also created opportunities for cyber offenders to engage in intimidation, harassment, bullying and invasion of privacy through online means.

Cyber stalking refers to the repeated use of digital communication technologies to monitor, threaten, harass or intimidate an individual. Such conduct may include persistent messaging, online surveillance, unauthorized access to social media accounts, circulation of morphed images and tracking of personal activities through digital platforms. In many cases, victims experience severe psychological distress, fear and reputational harm as a result of continuous online harassment.

[15] Vakul Sharma, Information Technology Law and Practice (Universal Law Publishing 2011).

Women and minors are particularly vulnerable to cyber stalking and online abuse. Incidents involving **revenge pornography, fake social media profiles, morphing of photographs, online blackmail and sexually explicit harassment** have increased substantially in recent years. Cyber offenders frequently misuse digital anonymity to target victims while avoiding identification and legal consequences.[16]

In India, cyber stalking and online harassment are addressed under the **Information Technology Act, 2000** and relevant provisions of the **Bharatiya Nyaya Sanhita, 2023** relating to stalking, obscenity, criminal intimidation and publication of sexually explicit material. Judicial recognition of privacy and dignity under **Justice K. S. Puttaswamy v. Union of India** has further *strengthened constitutional protection against digital harassment and unauthorized intrusion into personal life*.[17]

6. Cryptocurrency and Dark Web Crimes:

The rapid growth of **cryptocurrency transactions and dark web networks** has created new challenges for cyber security and criminal law enforcement in India. Although digital currencies and anonymous online platforms were originally developed for technological innovation and privacy, they have increasingly been misused for illegal financial transactions, cyber fraud, money laundering and organized cyber-criminal activities.

Cryptocurrency refers to decentralized digital currency that operates through blockchain technology without direct control of a central authority. Transactions involving cryptocurrencies such as Bitcoin and Ethereum often provide a significant degree of anonymity, making them attractive for cyber criminals engaged in illegal online activities. Cyber offenders frequently use cryptocurrency for ransomware payments, online fraud, illegal trade and concealment of proceeds generated through Cyber-crimes.

Another major concern is the growing use of the **dark web**, which refers to hidden internet networks accessible only through specialized software such as Tor browsers. Unlike the ordinary internet, dark web platforms provide a high level of anonymity to users and are frequently used for unlawful activities including sale of stolen data, hacking tools, counterfeit documents, narcotic substances and illegal digital content.

[16] National Cyber Crime Reporting Portal, https://cybercrime.gov.in (last visited May 28, 2026).
[17] Justice K.S. Puttaswamy (Retd.) v. Union of India, (2017) 10 SCC 1.

Cyber criminals often use dark web marketplaces to purchase and sell **stolen personal information, bank account details, malware software and hacking services**. Large scale data breaches are frequently followed by illegal sale of sensitive information on dark web platforms. Such activities not only facilitate financial fraud, but also contribute to identity theft, cyber espionage and organized transnational cyber-crime.

In India, cyber offences involving cryptocurrency and dark web activities are addressed through provisions under the **Information Technology Act, 2000**, the **Prevention of Money Laundering Act, 2002** and relevant provisions of the **Bharatiya Nyaya Sanhita, 2023**. However, the absence of a comprehensive regulatory framework governing cryptocurrency transactions continues to create legal uncertainty and enforcement difficulties.[18]

7. Cyber Terrorism and Threats to National Security:

The increasing dependence upon digital infrastructure has significantly expanded the risk of **cyber terrorism and cyber-attacks against national security**. In the modern era, cyber space has become a strategic domain where hostile actors, terrorist organizations and foreign cyber groups can target critical infrastructure, government systems and public institutions without engaging in conventional warfare. As a result, cyber security is no longer merely a technological concern, but an essential component of national security and public safety.

Cyber terrorism generally refers to the use of computer networks, digital systems or online platforms to cause large scale disruption, fear or damage for political, ideological or terrorist objectives. Such attacks may target banking systems, defence networks, communication infrastructure, transportation systems, power grids or government databases. The objective is often to create panic, disrupt essential services and weaken public confidence in State institutions.

One of the most serious concerns relating to cyber terrorism is the possibility of attacks on **critical information infrastructure**. Cyber-attacks on electricity grids, healthcare systems, airports, defence communications or financial institutions may paralyze essential services and create severe economic and social consequences. In highly digitized societies, even temporary disruption of digital infrastructure can significantly affect governance and national stability.

Terrorist organizations and hostile cyber groups increasingly use digital platforms for **online radicalization, encrypted communication, propaganda dissemination, recruitment and**

[18] National Crime Records Bureau, https://www.ncrb.gov.in (last visited May 28, 2026).

financial transactions. Social media and anonymous messaging applications are frequently misused for spreading extremist content and coordinating unlawful activities across borders. The use of cryptocurrency and dark web networks further complicates monitoring and investigation of such activities.[19]

LEGAL FRAMEWORK GOVERNING CYBER-CRIMES IN INDIA

Information Technology Act, 2000:

The **Information Technology Act, 2000** is the primary legislation governing Cyber-crimes and electronic commerce in India. Enacted to provide legal recognition to electronic records and digital transactions, the Act also establishes criminal liability for various cyber offences committed through computers and digital networks. Over time, the Act has become the foundation of India's cyber law regime and plays a crucial role in regulating cyber security related offences.

One of the most important provisions under the Act is **Section 43**, which imposes civil liability for unauthorized access, downloading of data, introduction of viruses and disruption of computer systems. The provision aims to protect computer resources and digital infrastructure from unlawful interference and cyber-attacks.[20]

The Act further criminalizes hacking and dishonest cyber activities through **Section 66**, which provides punishment for unauthorized access and damage caused to computer systems.[21] In addition, **Section 66C** specifically addresses identity theft involving misuse of passwords, digital signatures and unique identification information,[22] while **Section 66D** punishes cheating by personation through computer resources and online communication.[23]

Another significant provision is **Section 67**, which penalizes publication and transmission of obscene material in electronic form. The law also contains stricter provisions relating to sexually explicit content and child sexual abuse material circulated through digital platforms.[24]

With increasing concerns regarding cyber terrorism and national security, the Information Technology Act introduced **Section 66F**,[25] which criminalizes cyber terrorism involving

[19] R. K. Chaubey, Emerging Challenges of Cyber Crimes in India, 8 Int'l J. Legal Stud. 112 (2022).
[20] Information Technology Act, No. 21 of 2000, § 43, INDIA CODE (2000).
[21] Information Technology Act, No. 21 of 2000, § 66, INDIA CODE (2000).
[22] Information Technology Act, No. 21 of 2000, § 66C, INDIA CODE (2000).
[23] Information Technology Act, No. 21 of 2000, § 66D, INDIA CODE (2000).
[24] Information Technology Act, No. 21 of 2000, § 67, INDIA CODE (2000).
[25] Information Technology Act, No. 21 of 2000, § 66F, INDIA CODE (2000).

attacks on critical information infrastructure and activities threatening the sovereignty, integrity and security of India. The Act further empowers the government under **Section 69** to intercept, monitor and decrypt information under certain circumstances involving national security and public order.[26]

The protection of critical digital infrastructure is addressed through **Section 70**, which authorizes the government to declare certain computer systems as protected systems and impose restrictions against unauthorized access.[27] Institutions such as **CERT-In** have also been established to respond to cyber security incidents and strengthen national cyber resilience.

Bharatiya Nyaya Sanhita, 2023:

The **Bharatiya Nyaya Sanhita, 2023** has replaced the Indian Penal Code, 1860 and now functions as the primary substantive criminal law legislation in India. Although cyber offences are mainly governed by the **Information Technology Act, 2000**, several cyber related activities such as **online cheating, identity theft, cyber stalking, digital intimidation and fraudulent impersonation** may also attract criminal liability under the BNS.

With the increasing use of digital platforms for criminal activities, traditional criminal law provisions have become increasingly relevant in addressing technology-based offences.

The emergence of **AI generated frauds, deepfake manipulation, online harassment and digital financial scams** has further expanded the role of criminal law within cyber regulation. Cyber criminals frequently misuse digital technologies for extortion, fake identities and circulation of manipulated electronic content causing reputational and financial harm.

Although the BNS does not specifically regulate all emerging cyber threats in detail, its provisions relating to cheating, forgery, obscenity and intimidation continue to supplement the legal framework governing cyber-crimes in India.

Digital Personal Data Protection Act, 2023:

The **Digital Personal Data Protection Act, 2023** was enacted to regulate the collection, processing and protection of digital personal data in India. The legislation recognizes the growing importance of informational privacy in the digital era and imposes obligations upon entities handling personal data. The Act aims to protect individuals from unauthorized use,

[26] Information Technology Act, No. 21 of 2000, § 69, INDIA CODE (2000).
[27] Information Technology Act, No. 21 of 2000, § 70, INDIA CODE (2000).

disclosure and misuse of sensitive personal information while balancing the need for lawful data processing and digital innovation.

The enactment of the DPDP Act became particularly significant after the Supreme Court's decision in **Justice K. S. Puttaswamy v. Union of India**, which recognized privacy as a fundamental right under the Constitution. The Act introduces responsibilities relating to consent, data security and breach notification, while also providing penalties for non-compliance. However, concerns continue to exist regarding enforcement mechanisms, State exemptions and the adequacy of safeguards against mass surveillance and unauthorized data collection.

Role of CERT-In and Cyber Crime Portals:

The **Indian Computer Emergency Response Team (CERT-In)** functions as the national agency responsible for responding to cyber security incidents and strengthening cyber resilience in India. Established under the Information Technology Act, 2000, CERT-In monitors cyber threats, issues security advisories and coordinates responses to cyber-attacks affecting government institutions, private organizations and digital infrastructure. The agency plays an important role in preventing cyber intrusions, handling data breaches and improving national cyber security preparedness.[28]

In addition to CERT-In, the Government of India has also established the **National Cyber Crime Reporting Portal** to facilitate online reporting of cyber offences. The portal enables victims to report incidents relating to online financial fraud, cyber harassment, identity theft and other digital crimes in a more accessible and efficient manner. These institutional mechanisms have improved cyber-crime reporting and awareness; however, concerns regarding delayed investigation, lack of technical expertise and increasing cyber threats continue to challenge effective cyber law enforcement in India.

CHALLENGES IN INVESTIGATION AND ENFORCEMENT

(1) Jurisdictional Challenges

Cyber-crimes often involve multiple countries simultaneously, making it difficult to determine territorial jurisdiction. Differences between international legal systems frequently delay investigation and prosecution.

[28] Indian Computer Emergency Response Team (CERT-In), https://www.cert-in.org.in (last visited May 28, 2026).

(2) Anonymity of Cyber Criminals

Cyber offenders commonly use **VPN services, fake IP addresses and encrypted networks** to conceal their identity. This makes tracing and identification extremely difficult for investigative agencies.

(3) Problems Relating to Digital Evidence

Cyber offences primarily involve electronic evidence such as **server logs, metadata and digital records**. Preservation, collection and admissibility of such evidence remain major legal challenges.

(4) Lack of Technical Expertise

Many law enforcement agencies still lack adequate training and cyber forensic expertise required for investigating technologically sophisticated cyber offences.

(5) Rapid Technological Advancement

Cyber-crime techniques evolve faster than legal and regulatory mechanisms. Emerging threats such as **AI generated frauds and deepfake technology** continue to expose legislative gaps.

(6) Cross Border Cyber-crimes

Cyber-attacks frequently originate from foreign jurisdictions, creating practical difficulties in extradition, evidence collection and international coordination.

(7) Encryption and Dark Web Challenges

Encrypted communication systems and dark web platforms provide anonymity to offenders and complicate cyber surveillance and investigation processes.

(8) Low Reporting of Cyber-crimes

Many victims fail to report cyber offences due to lack of awareness, fear of reputational harm and limited trust in enforcement mechanisms.

JUDICIAL TRENDS AND LANDMARK DECISIONS

1. Shreya Singhal v. Union of India (2015)

In this landmark judgment, the Supreme Court struck down **Section 66A of the Information Technology Act, 2000** on the ground that it violated freedom of speech and expression under

Article 19(1)(a) of the Constitution. The decision strengthened protection against arbitrary restrictions on online expression.[29]

2. **Anvar P.V. v. P.K. Basheer (2014)**

The Supreme Court clarified the rules relating to **admissibility of electronic evidence** under the Indian Evidence Act. The Court held that electronic records must satisfy statutory requirements in order to be admissible during trial.[30]

3. **Justice K. S. Puttaswamy v. Union of India (2017)**

The Supreme Court recognized the **Right to Privacy as a fundamental right** under Articles 14, 19 and 21 of the Constitution. The judgment became the constitutional foundation for digital privacy and data protection jurisprudence in India.[31]

4. **Faheema Shirin v. State of Kerala (2019)**

The Kerala High Court observed that access to the internet forms part of the **Right to Education and Right to Privacy** under Article 21. The decision highlighted the growing constitutional importance of digital access in modern society.[32]

5. **Google India Pvt. Ltd. v. Visaka Industries (2020)**

The Supreme Court discussed the liability of online intermediaries and emphasized the importance of balancing freedom of speech with accountability for unlawful online content.[33]

Through constitutional interpretation and recognition of digital rights, Indian courts have significantly contributed towards strengthening the legal framework governing cyber space.

CRITICAL ANALYSIS OF INDIA'S CYBER LAW REGIME

- **Outdated Nature of the Information Technology Act, 2000:**

Although the Information Technology Act forms the foundation of cyber law in India, several of its provisions are inadequate to address modern cyber threats such as **AI generated frauds, deepfake technology and cryptocurrency crimes**.

[29] Shreya Singhal v. Union of India, (2015) 5 SCC 1.
[30] Anvar P.V. v. P.K. Basheer, (2014) 10 SCC 473.
[31] Justice K.S. Puttaswamy (Retd.) v. Union of India, (2017) 10 SCC 1.
[32] Faheema Shirin v. State of Kerala, 2019 SCC OnLine Ker 1733.
[33] Google India Pvt. Ltd. v. Visaka Industries Ltd., (2020) 4 SCC 162.

- **Rapid Growth of AI Based Cyber Threats:**

Artificial intelligence has significantly increased the sophistication of cyber offences. Existing legal frameworks still lack comprehensive regulation relating to AI driven Cyber-crimes and automated digital frauds.

- **Weak Enforcement Mechanisms:**

Despite the existence of cyber laws, effective enforcement remains difficult due to shortage of trained cyber experts, delayed investigation and lack of advanced cyber forensic infrastructure.

- **Low Conviction Rates:**

Cyber-crime cases often involve technical complexity, jurisdictional issues and evidentiary challenges, resulting in comparatively low conviction rates and weak deterrence.

- **Concerns Relating to Privacy and Surveillance:**

Measures adopted for cyber security and digital monitoring may sometimes conflict with the constitutional right to privacy recognized in Justice K. S. Puttaswamy v. Union of India.

- **Increasing Role of Private Technology Corporations:**

Large technology companies collect and process massive amounts of personal data. Weak regulation of corporate data handling practices continues to create concerns regarding misuse of personal information.

- **Lack of Public Awareness:**

A significant portion of cyber offences succeed due to lack of cyber awareness and digital literacy among users, particularly in cases involving phishing and online financial fraud.

- **Need for International Cooperation:**

The borderless nature of Cyber-crimes makes international cooperation essential. However, differences between national legal systems often delay investigation and enforcement processes.

- **Absence of Specialized Cyber Courts:**

India still lacks sufficient specialized cyber courts and dedicated digital adjudication mechanisms capable of handling technologically complex cyber disputes efficiently.

- **Need for Continuous Legal Modernization:**

Cyber-crimes evolve rapidly alongside technological advancement. Consequently, cyber laws and regulatory mechanisms must continuously adapt to emerging digital threats and technological innovation.

SUGGESTIONS AND REFORMS

a. Strengthening Cyber Security Infrastructure

India must develop stronger cyber security systems capable of detecting and preventing sophisticated cyber-attacks on digital infrastructure and financial networks.

b. Specialized Cyber Crime Training

Regular technical training should be provided to police officers, investigators and judicial authorities dealing with cyber offences and digital evidence.

c. AI Specific Legal Regulation

The government should introduce clearer legal frameworks regulating **artificial intelligence, deepfake technology and automated cyber frauds**.

d. Establishment of Specialized Cyber Courts

Dedicated cyber courts and fast track digital adjudication mechanisms should be established for speedy disposal of cyber-crime cases.

e. Enhancing Public Awareness and Digital Literacy

Public awareness campaigns relating to **online fraud, phishing, cyber safety and digital privacy** should be strengthened at both educational and institutional levels.

f. Improved International Cooperation

India should strengthen international collaboration for information sharing, extradition and coordinated investigation of cross border cyber-crimes.

g. Strengthening Data Protection Mechanisms

More effective safeguards should be implemented for protection of personal data and prevention of unauthorized digital surveillance.

CONCLUSION

The rapid growth of digital technology has significantly transformed modern society, but it has simultaneously increased the scale and complexity of Cyber-crimes in India. Offences such as **phishing, identity theft, ransomware attacks, deepfake frauds, cyber stalking and cryptocurrency related crimes** demonstrate that cyber threats are evolving alongside technological advancement. These offences not only affect financial security and individual privacy, but also pose serious risks to national security, public confidence and digital governance.

The author is of the opinion that India's existing cyber law framework, particularly the **Information Technology Act, 2000**, has played an important role in regulating cyber offences, but rapid technological development has exposed several legislative and enforcement gaps. Emerging technologies such as **artificial intelligence, automated cyber-attacks and deepfake systems** require stronger and more adaptive legal responses capable of addressing contemporary digital threats effectively.

In the words of **Justice D. Y. Chandrachud**, **"Privacy is the constitutional core of human dignity."**[34] The future effectiveness of India's cyber law regime will ultimately depend upon whether constitutional institutions, legislative authorities and enforcement agencies are capable of protecting both digital security and fundamental rights in an increasingly interconnected technological society.

REFERENCES

BOOKS

- Aparna Viswanathan, *Cyber Law: Indian and International Perspectives on Key Topics Including Data Security, E-Commerce and Cloud Computing* (LexisNexis 2012).
- Karnika Seth, *Computers, Internet and New Technology Laws* (LexisNexis 2013).
- Talwant Singh, *Cyber Law and Information Technology* (Allahabad Law Agency 2021).
- Vakul Sharma, *Information Technology Law and Practice* (Universal Law Publishing 2011).

[34] Justice K.S. Puttaswamy (Retd.) v. Union of India, (2017) 10 SCC 1, 497 (per Chandrachud, J.).

STATUTES

- Bharatiya Nyaya Sanhita, 2023.
- Digital Personal Data Protection Act, 2023.
- Information Technology Act, 2000.

CASES

- *Anvar P.V. v. P.K. Basheer*, (2014) 10 SCC 473.
- *Faheema Shirin v. State of Kerala*, 2019 SCC OnLine Ker 1733.
- *Google India Pvt. Ltd. v. Visaka Industries Ltd.*, (2020) 4 SCC 162.
- *Justice K.S. Puttaswamy (Retd.) v. Union of India*, (2017) 10 SCC 1.
- *Shreya Singhal v. Union of India*, (2015) 5 SCC 1.

JOURNAL ARTICLES

- Anubha Gupta, Cyber Crimes and Need for Strong Cyber Security Laws in India, 12 Indian J.L. & Tech. 45 (2021).
- R. K. Chaubey, Emerging Challenges of Cyber Crimes in India, 8 Int'l J. Legal Stud. 112 (2022).
- S. K. Verma, Artificial Intelligence and Cyber Security Challenges in India, 15 J. Digital L. & Pol'y 67 (2023).
- Maria Bada & Jason R. C. Nurse, Profiling the Cybercriminal: A Systematic Review of Research (2021).
- Lavanya Elluri et al., Recent Advancements in Machine Learning for Cybercrime Prediction (2023).
- Mariam Nouh, Jason R. C. Nurse, Helena Webb & Michael Goldsmith, Cybercrime Investigators are Users Too! Understanding the Socio-Technical Challenges Faced by Law Enforcement (2019).
- N. S. Nappinai, Cyber Crime Law in India: Has Law Kept Pace with Emerging Trends? An Empirical Study (2010).

WEB SOURCES

- Indian Computer Emergency Response Team (CERT-In), https://www.cert-in.org.in (last visited May 28, 2026).
- Ministry of Electronics and Information Technology, Government of India, https://www.meity.gov.in (last visited May 28, 2026).
- National Cyber Crime Reporting Portal, https://cybercrime.gov.in (last visited May 28, 2026).
- National Crime Records Bureau, https://www.ncrb.gov.in (last visited May 28, 2026).