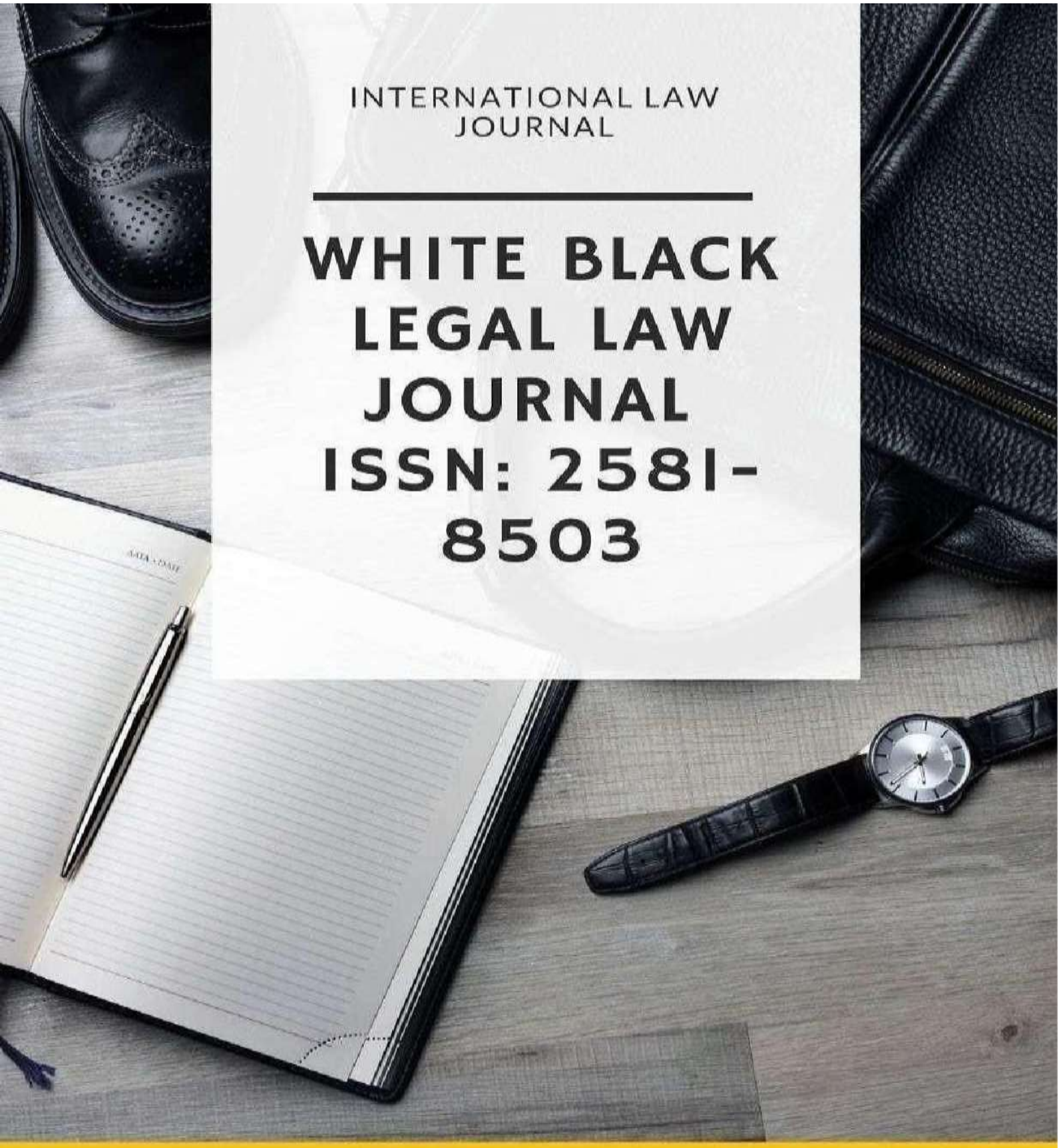

INTERNATIONAL LAW JOURNAL

WHITE BLACK LEGAL LAW JOURNAL

ISSN: 2581-8503

Peer - Reviewed & Refereed Journal

The Law Journal strives to provide a platform for discussion of International as well as National Developments in the Field of Law.

WWW.WHITEBLACKLEGAL.CO.IN

DISCLAIMER

EDITORIAL TEAM

Raju Narayana Swamy (IAS) Indian Administrative Service officer

Dr. Raju Narayana Swamy popularly known as Kerala's Anti-Corruption Crusader is the All India Topper of the 1991 batch of the IAS and is currently posted as Principal Secretary to the Government of Kerala. He has earned many accolades as he hit against the political-bureaucrat corruption nexus in India. Dr Swamy holds a B.Tech in Computer Science and Engineering from the IIT Madras and a Ph. D. in Cyber Law from Gujarat National Law University. He also has an LLM (Pro) (with specialization in IPR) as well as three PG Diplomas from the National Law University, Delhi- one in Urban Environmental Management and Law, another in Environmental Law and Policy and a third one in Tourism and Environmental Law. He also holds a post-graduate diploma in IPR from the National Law School, Bengaluru and a professional diploma in Public Procurement from the World Bank.

Dr. R. K. Upadhyay

Dr. R. K. Upadhyay is Registrar, University of Kota (Raj.), Dr Upadhyay obtained LLB , LLM degrees from Banaras Hindu University & Phd from university of Kota.He has succesfully completed UGC sponsored M.R.P for the work in the ares of the various prisoners reforms in the state of the Rajasthan.

Senior Editor

Dr. Neha Mishra

Dr. Neha Mishra is Associate Professor & Associate Dean (Scholarships) in Jindal Global Law School, OP Jindal Global University. She was awarded both her PhD degree and Associate Professor & Associate Dean M.A.; LL.B. (University of Delhi); LL.M.; Ph.D. (NLSIU, Bangalore) LLM from National Law School of India University, Bengaluru; she did her LL.B. from Faculty of Law, Delhi University as well as M.A. and B.A. from Hindu College and DCAC from DU respectively. Neha has been a Visiting Fellow, School of Social Work, Michigan State University, 2016 and invited speaker Panelist at Global Conference, Whitney R. Harris World Law Institute, Washington University in St.Louis, 2015.

Ms. Sumiti Ahuja

Ms. Sumiti Ahuja, Assistant Professor, Faculty of Law, University of Delhi,

Ms. Sumiti Ahuja completed her LL.M. from the Indian Law Institute with specialization in Criminal Law and Corporate Law, and has over nine years of teaching experience. She has done her LL.B. from the Faculty of Law, University of Delhi. She is currently pursuing Ph.D. in the area of Forensics and Law. Prior to joining the teaching profession, she has worked as Research Assistant for projects funded by different agencies of Govt. of India. She has developed various audio-video teaching modules under UGC e-PG Pathshala programme in the area of Criminology, under the aegis of an MHRD Project. Her areas of interest are Criminal Law, Law of Evidence, Interpretation of Statutes, and Clinical Legal Education.

Dr. Navtika Singh Nautiyal

Dr. Navtika Singh Nautiyal presently working as an Assistant Professor in School of law, Forensic Justice and Policy studies at National Forensic Sciences University, Gandhinagar, Gujarat. She has 9 years of Teaching and Research Experience. She has completed her Philosophy of Doctorate in 'Intercountry adoption laws from Uttranchal University, Dehradun' and LLM from Indian Law Institute, New Delhi.

Dr. Rinu Saraswat

Associate Professor at School of Law, Apex University, Jaipur, M.A, LL.M, Ph.D,

Dr. Rinu have 5 yrs of teaching experience in renowned institutions like Jagannath University and Apex University. Participated in more than 20 national and international seminars and conferences and 5 workshops and training programmes.

Dr. Nitesh Saraswat

E.MBA, LL.M, Ph.D, PGDSAPM
Currently working as Assistant Professor at Law Centre II, Faculty of Law, University of Delhi. Dr. Nitesh have 14 years of Teaching, Administrative and research experience in Renowned Institutions like Amity University, Tata Institute of Social Sciences, Jai Narain Vyas University Jodhpur, Jagannath University and Nirma University.
More than 25 Publications in renowned National and International Journals and has authored a Text book on Cr.P.C and Juvenile Delinquency law.

Subhrajit Chanda

BBA. LL.B. (Hons.) (Amity University, Rajasthan); LL. M. (UPES, Dehradun) (Nottingham Trent University, UK); Ph.D. Candidate (G.D. Goenka University)

Subhrajit did his LL.M. in Sports Law, from Nottingham Trent University of United Kingdoms, with international scholarship provided by university; he has also completed another LL.M. in Energy Law from University of Petroleum and Energy Studies, India. He did his B.B.A.LL.B. (Hons.) focussing on International Trade Law.

ABOUT US

WHITE BLACK LEGAL is an open access, peer-reviewed and refereed journal providededicated to express views on topical legal issues, thereby generating a cross current of ideas on emerging matters. This platform shall also ignite the initiative and desire of young law students to contribute in the field of law. The erudite response of legal luminaries shall be solicited to enable readers to explore challenges that lie before law makers, lawyers and the society at large, in the event of the ever changing social, economic and technological scenario.

With this thought, we hereby present to you

www.whiteblacklegal.co.in
Volume 3 Issue 2 | July 2025 ISSN: 2581-8503

CYBERCRIME AND THE LAW: ADDRESSING THE CHALLENGES OF DIGITAL OFFENSES IN INDIA

AUTHORED BY - ANKIT KUMAR SINGH.

Introduction

In the digital age, the emergence of cybercrime represents one of the most profound challenges to legal systems globally. India, with its rapidly growing digital ecosystem and expanding internet user base, has seen a surge in digital offenses ranging from financial fraud and identity theft to cyberterrorism and cyberbullying. The legal framework in India, although evolving, often lags behind the rapidly mutating techniques used by cybercriminals. This paper examines the nature of cybercrime in India, evaluates the legal responses, and explores the gaps and enforcement challenges that persist despite legislative advancements.

1. Understanding Cybercrime

1.1 Defining Cybercrime

Cybercrime refers to unlawful activities that involve computers, digital devices, or online networks either as the instrument, the target, or the environment in which the crime takes place. It constitutes a broad array of offences, ranging from unauthorized access to computer systems (commonly referred to as hacking), phishing scams, identity theft, ransomware attacks, and cyberbullying, to more egregious crimes such as child sexual exploitation and cyberterrorism. The borderless nature of cyberspace allows these crimes to be committed with anonymity, scale, and speed, thereby posing unique legal and enforcement challenges.

In India, the **Information Technology Act, 2000**, as amended by the **Information Technology (Amendment) Act, 2008**, is the primary legal instrument that addresses digital offences. However, the Act lacks a singular, overarching definition of "cybercrime." Instead, it identifies and criminalizes specific forms of misconduct involving digital technologies. Notable among these are Section 66 (computer-related offences), Section 66C (identity theft), Section 66D (cheating by personation using computer resources), Section 66E (violation of privacy), and Section 67 (publishing or transmitting obscene material in electronic form). While these provisions serve as foundational elements in the cybercrime jurisprudence of India, the absence

of a consolidated statutory definition continues to result in interpretative ambiguities.

1.2 Categories of Cybercrime

Cybercrime in the Indian context can be broadly categorized into three main types based on the target of the criminal activity: (i) cybercrimes against individuals, (ii) cybercrimes against property, and (iii) cybercrimes against government or society.

(i) Cybercrimes against Individuals

These offenses are primarily aimed at causing psychological, emotional, reputational, or financial harm to specific individuals. Common examples include:

- **Cyberstalking**: The use of the internet or other electronic means to stalk or harass an individual, group, or organization.
- **Online defamation**: Publishing false or defamatory statements about a person with the intent to damage their reputation.
- **Identity theft**: Illegally obtaining and misusing another person's personal information, such as Aadhaar numbers, bank details, or login credentials.
- **Sextortion and cyberbullying**: Using sexually explicit material to coerce victims or using digital platforms to harass or intimidate.

The legal remedies for such offences are often scattered across both the IT Act and provisions of the **Indian Penal Code, 1860** (now largely codified in the **Bharatiya Nyaya Sanhita, 2023**), such as defamation, criminal intimidation, and obscenity.

(ii) Cybercrimes against Property

These offences involve targeting digital infrastructure, data, or intangible property belonging to individuals, businesses, or institutions. Examples include:

- **Hacking**: Unauthorized access to computer systems to manipulate, destroy, or steal data.
- **Phishing and spoofing**: Fraudulently acquiring sensitive information by impersonating legitimate institutions.
- **Ransomware attacks**: Encrypting an entity's digital assets and demanding a ransom for decryption.
- **Intellectual property theft**: Illegally copying or distributing copyrighted software, music, books, or trademarks.

With the increasing digitization of business and government services, the economic consequences of these crimes can be catastrophic. Sections such as 43 (unauthorized access and damage to systems) and 66 (computer-related offenses) of the IT Act provide for civil and

criminal liability in such cases.

(iii) Cybercrimes against Government or Society

These involve digital acts that threaten national security, public safety, or public order. These include:

- **Cyberterrorism**: The use of cyberspace to incite terror, target critical information infrastructure, or disrupt essential services.
- **Attacks on government networks**: Unauthorized intrusion into military, judicial, or administrative digital infrastructure.
- **Misinformation and fake news campaigns**: The deliberate spread of false information via social media to incite communal tensions, discredit institutions, or manipulate elections.

Section 66F of the IT Act specifically criminalizes cyberterrorism, prescribing stringent penalties including life imprisonment. In cases where national sovereignty or public order is threatened, additional charges under the **Unlawful Activities (Prevention) Act, 1967**, or the **Official Secrets Act, 1923** may also be invoked.

2. Legal Framework for Cybercrime in India

India's legal framework to combat cybercrime comprises a combination of general criminal law, technology-specific statutes, and sectoral regulations. While the **Information Technology Act, 2000** (IT Act) is the cornerstone of digital crime regulation, the **Indian Penal Code, 1860** (now largely replaced by the **Bharatiya Nyaya Sanhita, 2023**), sector-specific guidelines, and data protection statutes play critical supplementary roles.

2.1 The Information Technology Act, 2000

The **Information Technology Act, 2000**, enacted to provide legal recognition to electronic records and digital signatures, was substantially amended in **2008** to address emerging cyber threats. It remains the principal statute addressing cybercrime in India.

Key penal provisions under the IT Act include:

- **Section 43**: Imposes civil liability for unauthorized access, data theft, or virus attacks.
- **Section 66**: Criminalizes acts under Section 43 when done dishonestly or fraudulently.
- **Section 66C**: Deals with **identity theft**, i.e., fraudulent use of digital signatures, passwords, or biometric data.

- **Section 66D**: Addresses **cheating by personation using computer resources**, often invoked in phishing or UPI fraud cases.
- **Section 66E**: Prohibits **violation of privacy**, including capturing or transmitting private images without consent.
- **Sections 67, 67A, 67B**: Criminalize publication and transmission of **obscene**, **sexually explicit**, or **child sexual abuse material (CSAM)** in electronic form.
- **Section 66F**: Defines and penalizes **cyberterrorism**, including unauthorized access to critical information infrastructure that threatens sovereignty or integrity of India.

Judicial Insight: In *Shreya Singhal v. Union of India*, the Supreme Court struck down Section 66A (which criminalized offensive messages online) as unconstitutional for violating free speech.[1]

Note: The IT Act does not provide a comprehensive definition of "cybercrime" but addresses specific offenses and penalties in Chapters IX and XI.

2.2 Indian Penal Code, 1860 and Bharatiya Nyaya Sanhita, 2023

Despite the specificity of the IT Act, many cybercrimes are prosecuted under general criminal provisions of the **Indian Penal Code, 1860 (IPC)**. With the introduction of the **Bharatiya Nyaya Sanhita, 2023 (BNS)**, several offenses have been retained or updated to accommodate cyber-related conduct.

Commonly invoked provisions include:

Offense	IPC Provision	Corresponding BNS Section
Cheating by impersonation	Section 419	Section 315
Cheating and fraudulent inducement	Section 420	Section 316
Criminal intimidation	Section 506	Section 351
Stalking (including online)	Section 354D	Section 73
Defamation (including digital)	Section 499	Section 356
Extortion	Section 384	Section 309

Procedural Improvements in BNS, 2023:

- Introduces faster investigation deadlines.

[1] *Shreya Singhal v Union of India* (2015) 5 SCC 1 (SC).

- Enhances provisions related to **digital evidence** and cyber offenses.
- Allows for video recording of search and seizure operations (Section 105 BNS) in digital investigations.

The IPC/BNS provisions are often used alongside IT Act provisions for hybrid crimes such as **cyberstalking with threats**, **online financial fraud**, or **morphing images for blackmail**.

2.3 Sector-Specific and Supplementary Laws

India's cybercrime legal framework is bolstered by sectoral regulations and data protection laws that impose specific obligations on intermediaries, financial institutions, and data fiduciaries.

Sensitive Personal Data or Information (SPDI) Rules, 2011

Formulated under **Section 43A of the IT Act**, these rules define "sensitive personal data" and impose requirements on corporate entities regarding consent, data security, and disclosure.

CERT-In Directions, 2022

Issued by the **Indian Computer Emergency Response Team (CERT-In)** under Section 70B of the IT Act, these directions mandate:

- Reporting of cyber incidents within **6 hours** of detection.
- **Retention of logs for 180 days** by intermediaries and service providers.
- Maintenance of KYC and data records by VPN providers and data centers.

Digital Personal Data Protection Act, 2023 (DPDPA)

The DPDPA governs the processing of personal data by **data fiduciaries** and **data processors**. It introduces:

- Purpose limitation and data minimization principles.
- Consent-based processing.
- Penalties up to ₹250 crore for data breaches.
- Establishment of the **Data Protection Board of India** for adjudication.

Sectoral Regulations

- **RBI's Cybersecurity Framework (2016)** mandates **cyber incident reporting**, **board-level oversight**, and **vulnerability assessments** for banks.
- **SEBI's Guidelines (2015, revised 2022)** enforce cybersecurity audits and breach disclosures for stock exchanges, brokers, and depositories.

Legal Basis:

- RBI's directions issued under **Section 35A of the Banking Regulation Act, 1949**.
- SEBI circulars under powers derived from **SEBI Act, 1992**.

3. Enforcement Challenges in Prosecuting Cybercrime in India

India's legal and institutional response to cybercrime is evolving, but significant enforcement challenges persist. Despite a growing digital economy and increasing cyberthreats, the prosecution of cybercrimes in India is impeded by jurisdictional issues, technical deficits, low reporting rates, and procedural bottlenecks in digital evidence handling.

3.1 Jurisdictional Complexities

A defining feature of cybercrime is its transnational nature. Criminals can operate from outside Indian territory while targeting systems, networks, or individuals located within India. This raises serious issues of **territorial jurisdiction** under Indian criminal law.

Under **Section 75 of the Information Technology Act, 2000**, the Act has **extraterritorial application**, stating that it applies to any offense committed **outside India** if it involves a **computer, computer system or network located in India**. Similarly, **Section 4 of the Indian Penal Code, 1860 (now Section 4 of Bharatiya Nyaya Sanhita, 2023)** also provides for extraterritorial jurisdiction in specific cases.

Challenge: Despite these provisions, enforcement is contingent on:

- Accessing evidence located on foreign servers.
- Cooperation from foreign entities, including tech companies.
- Legal assistance from foreign governments through **Mutual Legal Assistance Treaties (MLATs)** or **Letters Rogatory**.

As of 2025, India has MLATs with over 40 countries, but delays in execution are common, often stretching to several months or years. Additionally, India is **not a party to the Budapest Convention on Cybercrime (2001)**, the only binding international treaty on cybercrime, which restricts seamless cross-border cooperation.

3.2 Lack of Technical Capacity

Despite the establishment of state cybercrime cells and specialized units, Indian law enforcement continues to suffer from:

- **Inadequate digital forensic infrastructure**, especially in Tier 2 and Tier 3 cities.
- **Shortage of trained cyber police officers** proficient in network analysis, dark web investigation, or reverse malware engineering.
- **Overburdened judicial officers** lacking specialized knowledge in data protection or digital evidence.

While the **Indian Cyber Crime Coordination Centre (I4C)** has attempted to bridge capacity gaps through training programs and model cyber forensic labs, implementation is uneven across states.

Government Efforts:

- The **Home Ministry's Cyber Crime Volunteer Program** (2020) under I4C enables citizens to report illegal content.
- The **Bureau of Police Research and Development (BPR&D)** runs capacity-building initiatives.
- National Forensic Sciences University (NFSU) in Gujarat offers advanced training, but scale remains a concern.

3.3 Low Reporting and Awareness

According to the **NCRB's Crime in India Report (2023)**, nearly **70% of cybercrimes go unreported**, especially in rural or semi-urban areas. Several factors contribute to this:

- **Lack of digital literacy**, particularly among senior citizens, women, and rural users.
- **Fear of social stigma**, especially in cases involving sextortion, cyberstalking, or image-based abuse.
- **Perceived inefficacy of police** in handling tech-intensive crimes.
- **Low trust in online complaint mechanisms**, despite the existence of the **National Cyber Crime Reporting Portal** (www.cybercrime.gov.in), launched in 2019.

Corrective Measures:

- Awareness campaigns by **CERT-In**, **NCW**, and NGOs like **CyberPeace Foundation**.
- Integration of cybersecurity awareness into the **Digital India** and **PMGDISHA** programs.

Yet, the absence of localized support cells for victims, especially women and minors, hinders effective grievance redressal.

3.4 Procedural and Evidentiary Hurdles

The **Indian Evidence Act, 1872**, was amended in 2000 and again in 2016 to incorporate provisions for the admissibility of **electronic records** (Section 65A and 65B). However, procedural implementation remains challenging:

- **Chain of custody** is not always maintained by investigating agencies, resulting in **integrity issues**.

- **Hash value generation**, essential for proving the immutability of digital files, is not standard practice across jurisdictions.
- **Lack of uniform digital forensic standards** or certified tools impacts evidence authenticity.
- **Metadata analysis** is often overlooked or misinterpreted in court proceedings.

Case Law Insight:

In *Anvar P.V. v. P.K. Basheer*, the Supreme Court held that **electronic records are admissible only if accompanied by a certificate under Section 65B(4)**.[2] The judgment underscored the importance of strict procedural compliance.

This ruling overruled the earlier position in **State (NCT of Delhi) v. Navjot Sandhu (2005)** (the Parliament Attack case), where secondary evidence like printouts and CDs were held admissible without a 65B certificate.[3]

Platform Delays:

Tech intermediaries like Meta, Google, and X (formerly Twitter) often resist sharing user data without court orders or invoke international data privacy standards (such as GDPR or their own policies), delaying investigations.

4. Recent Trends in Cybercrime in India

India's rapid digital transformation—spurred by initiatives like **Digital India**, the expansion of mobile internet, and the widespread adoption of fintech—has coincided with an unprecedented surge in cybercrime. The **National Crime Records Bureau (NCRB)** and **Indian Computer Emergency Response Team (CERT-In)** have reported year-on-year increases in sophisticated cyber threats targeting individuals, businesses, and government institutions.

4.1 Rise in Financial and Banking Fraud

The proliferation of **Unified Payments Interface (UPI)**, mobile banking, and QR code-based transactions has led to a dramatic increase in digital financial frauds. Offenders exploit users via:

- **Phishing attacks**: Fake emails or SMSes purporting to be from banks or government agencies (e.g., Income Tax Department) to harvest login details.

[2]Anvar P.V. v. P.K. Basheer (2014) 10 SCC 473.
[3]State (NCT of Delhi) v. Navjot Sandhu (2005) 11 SCC 600.

- **Vishing and OTP fraud**: Fraudsters impersonate officials to trick users into sharing one-time passwords (OTPs).
- **Malicious apps**: Fake versions of payment apps (e.g., Paytm, GPay) that steal data.

According to the **RBI Annual Report 2024**, cyber frauds in digital payments accounted for over ₹820 crore in losses. Similarly, CERT-In issued multiple alerts in 2023–24 regarding phishing campaigns targeting bank customers and government portals.

Legal Provisions:

- **Section 66D, IT Act**: Cheating by personation using computer resources.
- **Section 420, IPC / Section 316, BNS**: Cheating and dishonestly inducing delivery of property.

These offenses often go unreported due to small monetary loss or lack of awareness among rural users.

4.2 Ransomware and Malware Attacks

India is among the top five countries globally targeted by **ransomware attacks**, according to the **IBM X-Force Threat Intelligence Index 2024**. Notable trends include:

- Attacks on **hospitals**, **municipal corporations**, and **state IT systems**.
- Demand for ransom payments in **cryptocurrencies**, making the trail difficult to track.
- Use of advanced persistent threats (APTs) by **foreign actors**, especially from Russia, China, and North Korea.

In 2023, the **All India Institute of Medical Sciences (AIIMS) Delhi** suffered a major ransomware attack, leading to system outages for over a week.

Legal Tools Available:

- **Section 66, IT Act**: Damage to computer systems.
- **Section 66F, IT Act**: Cyberterrorism (in cases involving critical infrastructure).
- **Section 384, IPC / Section 309, BNS**: Extortion.

Despite legal tools, actual **prosecution remains rare** due to:

- Use of encrypted communication.
- Offshore hosting of command-and-control (C2) servers.
- Absence of formal extradition treaties with many source countries.

4.3 Online Harassment and Child Exploitation

Digital platforms are increasingly misused for **cyberstalking, sextortion, doxing**, and **child sexual abuse material (CSAM)**. Platforms like **Telegram, WhatsApp, Instagram**, and **dark**

web forums are often used to distribute such content.

CERT-In, along with **Interpol** and **NCPCR**, has noted increased cases of:

- Minors being coerced into sending explicit content.
- CSAM being traded in closed online groups.
- Women facing deepfake-based blackmail.

Applicable Legal Provisions:

- **Section 66E, IT Act**: Violation of privacy.
- **Sections 67, 67A, 67B, IT Act**: Publishing/transmitting obscene or sexually explicit content.
- **POCSO Act, 2012**: For CSAM involving minors.
- **Section 354D, IPC / Section 73, BNS**: Stalking, including online stalking.

Challenge: Encrypted messaging platforms resist law enforcement requests citing privacy and jurisdictional limitations.

4.4 Deepfakes and Misinformation

The use of **AI-generated deepfakes** and **misinformation campaigns** has become a serious threat to democratic processes and public order in India. These range from:

- **Fake videos of political leaders**, especially during elections.
- **Manipulated pornographic content** featuring women.
- **Social media posts inciting communal violence or hatred**.

For example, in 2024, a deepfake of a senior Union Minister delivering anti-national remarks went viral, leading to unrest before it was debunked. Similarly, **misinformation during elections** has become rampant through platforms like X (formerly Twitter), YouTube, and WhatsApp.

Applicable Legal Framework:

- **Section 67 IT Act**: For obscene material.
- **Section 505 IPC / Section 358 BNS**: Statements creating or promoting enmity, rumors.
- **Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021**: Mandate takedown and traceability.

Policy Gap: India lacks a dedicated statute on **deepfakes**, and the **proposed Digital India Act (still in draft as of 2025)** is expected to address this.

5. Institutional Responses

5.1 CERT-In and Cyber Coordination Centres

The Indian Computer Emergency Response Team (CERT-In) plays a crucial role in monitoring cyber threats and issuing advisories. In 2022, CERT-In issued stringent guidelines mandating 6-hour reporting windows for incidents and VPN data retention requirements.

The **Indian Cyber Crime Coordination Centre (I4C)**, launched by the Ministry of Home Affairs, provides a framework for handling cybercrime complaints and supports states with training, cyber forensic labs, and capacity building.

5.2 State Police Cyber Cells

Almost every Indian state now operates a cybercrime cell. The National Cybercrime Reporting Portal (www.cybercrime.gov.in) allows victims to register complaints online. However, response times vary, and quality of investigation remains inconsistent.

5.3 Role of Judiciary

Indian courts have played an important role in interpreting cyber laws and protecting constitutional rights in the digital realm. In *Shreya Singhal v. Union of India* (2015), the Supreme Court struck down Section 66A of the IT Act for violating free speech rights. Courts have also emphasized the need for data protection and privacy in multiple rulings following the landmark *Justice K.S. Puttaswamy* judgment (2017).

6. Gaps and the Need for Reform

India's legal and institutional framework for addressing cybercrime, though evolving, continues to face significant limitations due to technological complexity, jurisdictional challenges, and legislative inertia. Emerging forms of cyber threats, transnational criminal activity, and insufficient public awareness demand a systemic overhaul of the existing architecture. This section critically examines these gaps and the pressing need for reform.

6.1 Inadequate Legal Coverage

While the **Information Technology Act, 2000** (as amended) provides a base framework, it is increasingly insufficient to deal with the complexities of **21st-century cyber threats**. Current gaps include:

- **AI-generated content** (e.g., deepfakes, synthetic media): These are not explicitly criminalized under the IT Act or IPC/BNS.
- **Cryptocurrency-related crimes**: Scams involving virtual assets like Bitcoin or Ethereum remain outside the scope of regulatory clarity, with no specific provisions under criminal law.
- **Data brokering and surveillance capitalism**: The trade of personal data by unauthorized third parties is not explicitly prohibited, and penalties under the **Digital Personal Data Protection Act, 2023 (DPDPA)** do not always extend to such actors.

While courts have occasionally interpreted existing laws to penalize such offenses under general provisions (e.g., cheating, impersonation), this approach lacks **predictability and uniformity**.

Recommendation: India needs either:

- A **dedicated Cybercrime Code** consolidating all digital offenses, or
- A comprehensive chapter within the **Bharatiya Nyaya Sanhita, 2023**, modeled after international best practices like the **Budapest Convention on Cybercrime**.

6.2 Need for a Unified Enforcement Framework

Currently, India's cybercrime enforcement ecosystem is **fragmented**:

Agency	Role
State Police/Cyber Cells	Investigate local cases; often lack training or cyber forensic tools
CERT-In	Technical analysis and incident response; lacks criminal enforcement power
Sectoral Regulators	(e.g., RBI, SEBI) enforce compliance for institutions they regulate
DPBI	Handles data protection violations, not criminal offenses

This multiplicity creates **overlaps**, **coordination gaps**, and **delays**, especially in **multi-state or transnational cybercrimes**.

Recommendation:

- Creation of a **National Cyber Security Authority (NCSA)** through legislation.
- The NCSA could have **statutory authority to investigate, coordinate, and prosecute** cyber offenses in collaboration with state and central agencies.

- A model could be drawn from the **National Investigation Agency (NIA)** structure or the **UK's National Cyber Security Centre (NCSC)**.

6.3 International Cooperation

Cybercrimes frequently cross borders, necessitating robust **international legal and operational cooperation**. India's current tools include:

- **Mutual Legal Assistance Treaties (MLATs)**: Used for evidence gathering and cooperation. However, these are **slow, bureaucratic**, and often ineffective for time-sensitive cyber cases.
- **Interpol channels**: Available but underutilized in digital crime enforcement.
- **Non-membership in the Budapest Convention**: India has declined to join the **Budapest Convention on Cybercrime**, citing sovereignty concerns. While India's position emphasizes multilateralism through the **UN Ad Hoc Committee on Cybercrime**, this slows its ability to access real-time international support.

Recommendation:

- India should **reconsider its position on the Budapest Convention**, possibly by negotiating **reservations or declarations** protecting its interests.
- Bilateral arrangements with major digital economies (e.g., EU, US, Japan) for **expedited data access** and **law enforcement cooperation** are urgently needed.

6.4 Digital Literacy and Victim Support

While schemes like **Digital India** have improved access, digital literacy remains low—particularly among vulnerable populations such as **women, children, and the elderly**. The absence of structured awareness programs and support systems leaves victims exposed to further harm.

Key issues include:

- Victims of **cyberstalking**, **sextortion**, and **financial fraud** often **avoid reporting** due to fear of stigma, mistrust in law enforcement, or procedural delays.
- There is **no institutional framework** for mental health assistance or legal aid specifically tailored to cybercrime victims.

Recommendation:

- **Digital literacy programs** should be embedded into school and adult education curricula.
- Establish **Victim Support Cells** with:

- Cyber-aware counselors and legal aid providers.
- Integration with **Women's Helpline (181)**, **Childline (1098)**, and **Cybercrime Portal (cybercrime.gov.in)**.
- Coordination with the **DPBI** for data breaches and identity theft cases.

Best Practice Models:

- **Australia's eSafety Commissioner**
- **UK's Revenge Porn Helpline**

Conclusion

India's journey in addressing cybercrime is marked by progress and pitfalls. While the legislative framework has evolved with the IT Act, the IPC/BNS, and sectoral regulations, significant challenges persist in enforcement, technical capacity, jurisdiction, and international cooperation. In the coming years, India's success in safeguarding its cyberspace will depend not just on laws, but on the robust implementation of policies, collaboration among institutions, and the digital empowerment of its citizens. The future of cybersecurity and digital justice in India lies in striking the right balance between innovation, regulation, and rights protection.