CYBERCRIME JURISDICTION IN INDIA: BRIDGING THE GAP BETWEEN LEGAL AUTHORITY AND ENFORCEMENT REALITY

Aryansh Singh*

ABSTRACT

It has been found that due to the rapid digitisation of India[1], there has been fundamental change of the socio-economic and administration frameworks of India, as well as, there have been more sophisticated cyber threats facing the nation. This research paper is a critical analysis of the completeness of the Indian cybercrime structure, especially in terms of jurisdiction, evidence barrier, and inefficiency within institutions in handling transnational computer crimes. The paper examines the relationship between the Information Technology Act, 2000[2], the Bharatiya Nyaya Sanhita (2023), the Bharatiya Sakshya Adhiniyam (2023), and the Digital Personal Data Protection Act (2023) on the one hand and the evolving judicial interpretations on the other hand. It claims that the legal system in India is normatively inclusive, jurisdictionally broad, but procedurally limited and operationally disjointed. By including newer trends, e.g. AI-driven cybercrime, deep fake fraud, digital arrest scams, the introduction of global regulation activities like the UN Cybercrime Convention (2025), the paper shows the growing disparity between legal power and enforcement capacity. It suggests a multi-layered reform model to improve the legal harmonisation, the modernisation of the evidentiary system, the capacity of the institution, and the international cooperation through the doctrinal, comparative and empirical analysis. This study concludes that governance of cybercrime in India needs to be transformed into a shift between reactive and proactive, and technology-based legalism.

Keywords: Cybercrime, Bharatiya Nyaya Sanhita, Bharatiya Sakshya Adhiniyam, DPDP Act, UN Cybercrime Convention.

*BBA LLB, FIRST YEAR, INDIAN INSTITUTE OF MANAGEMENT, ROHTAK.

[1] World Economic Forum, Global Cybersecurity Outlook (latest).

[2] Information Technology Act 2000; Bharatiya Nyaya Sanhita 2023; Bharatiya Sakshya Adhiniyam 2023; Digital Personal Data Protection Act 2023.

INTRODUCTION

The digital revolution has made India one of the biggest internet ecosystems in the world, as it has over 900 million users and a growing digital economy. This has changed the world to ensure economic development, better governance, and connectivity. Nonetheless, this has also increased a corresponding increase in cybercrime, including financial fraud and identity theft, ransomware attacks, and giant data breaches.

Cyber offences do not respect territorial boundaries, as traditional crimes do.[3] One cyber event can have more than one jurisdiction- an offender can be based in a different country, servers can be in a different country, and victims can be based in a different country. This is essentially a critique of the classical law of territorial jurisdiction, which is the foundation of criminal law implementation.

India has addressed these challenges by a mixture of legislative actions, such as the Information Technology Act, 2000, and then followed by reforms under the Bharatiya Nyaya Sanhita (2023) and Bharatiya Sakshya Adhiniyam (2023).[4] Nonetheless, in spite of these developments, the results of enforcement are still poor, and the conviction rates are low, and the delays during the prosecution process are vast.

As it is argued in this paper, the Indian system of cybercrime has a strong, but poorly operationalised, doctrinal foundation. The difference between law and the reality of enforcement is caused by the jurisdictional ambiguity, the limitation of evidence, and institutional fragmentation.

CONCEPTUAL FRAMEWORK: CYBERCRIME AND JURISDICTION

Cybercrime refers to a broad category of offences involving digital systems, networks, or data. These include hacking, phishing, identity theft, cyberstalking, ransomware attacks, and online financial fraud. The defining feature of cybercrime is its borderless nature, which disrupts traditional legal frameworks based on physical geography. To address this, legal systems have developed expanded jurisdictional doctrines:

- **Territorial Principle:** Jurisdiction based on the location of the offence.

[3] Cedric Ryngaert, Jurisdiction in International Law (2nd edn, OUP 2015).
[4] Information Technology Act 2000; Bharatiya Nyaya Sanhita 2023.

- **Nationality Principle:** Jurisdiction based on the offender's citizenship.
- **Passive Personality Principle:** Jurisdiction based on the victim's nationality.
- **Effects Doctrine:** Jurisdiction based on the impact within a state.
- **Protective Principle:** Jurisdiction over threats to national security.

India's cyber law framework incorporates elements of these doctrines, particularly through extraterritorial provisions under the IT Act and BNS. However, their practical application remains limited due to enforcement challenges.

LEGAL FRAMEWORK GOVERNING CYBERCRIME IN INDIA

Information Technology Act, 2000: India has a cyber law regime known as the IT Act.[5] It makes crimes like unauthorised access, data, identity fraud, and cyberterrorism. Section 75 also permits extraterritorial jurisdiction whereby Indian courts are empowered to try crimes that deal with computer systems situated in India, irrespective of the location of the crime.

Bharatiya Nyaya Sanhita (2023):[6] The BNS also substitutes the Indian Penal Code and also spreads criminal responsibility to offences carried out abroad that have domestic impacts. This is indicative of a change toward the realisation of the transnational aspect of cybercrime.

Bharatigala Sakshya Adhiniyam (2023):[7] BSA is seen to modernise the evidentiary law through the clear recognition of electronic records. It aims to overcome the drawbacks of previous provisions by broadening the admissibility models, even though there are practical issues related to the authentication of evidence across borders.

Digital Personal Data Protection Act, 2023:[8] DPDP Act brings in the obligations of data governance, breach reporting and data fiduciary accountability. Although it is mainly a privacy law, it enhances the prevention of cybercrime because it imposes more stringent requirements of data security.

[5] Information Technology Act 2000, s 75.
[6] Bharatiya Nyaya Sanhita 2023.
[7] Bharatiya Sakshya Adhiniyam 2023.
[8] Digital Personal Data Protection Act 2023.

JURISDICTIONAL CHALLENGES IN CYBERCRIME

Cybercrime creates complex jurisdictional dilemmas due to its inherently transnational nature. Determining the appropriate jurisdiction—whether based on the location of the offender, the server, or the victim—remains a significant challenge.

Although India asserts extraterritorial jurisdiction, enforcement depends on cooperation from foreign jurisdictions. Mechanisms such as Mutual Legal Assistance Treaties (MLATs) are often slow, resulting in delays that compromise digital evidence.[9]

Additionally, differences in legal definitions and standards across countries complicate extradition and prosecution. The principle of dual criminality further restricts cooperation in cases where conduct is not uniformly criminalised.

DIGITAL EVIDENCE AND PROCEDURAL CONSTRAINTS

Digital evidence is central to cybercrime prosecution but presents unique challenges:

- Volatility and ease of alteration
- Storage on foreign servers
- Dependence on third-party service providers
- Complex authentication requirements

Despite reforms under the BSA, evidentiary processes remain rigid. Cross-border data access is particularly problematic, as it requires navigating foreign legal systems and corporate policies.[10]

INSTITUTIONAL FRAMEWORK AND ENFORCEMENT GAPS

India's cybercrime enforcement involves multiple agencies, including CERT-In, the Indian Cyber Crime Coordination Centre (I4C), state cyber cells, and the Central Bureau of Investigation.[11] However, enforcement remains weak due to:

- Lack of coordination between agencies
- Insufficient technical expertise

[9] Malcolm N Shaw, International Law (8th edn, CUP 2017).
[10] Anvar PV v PK Basheer (2014) 10 SCC 473.
[11] CERT-In, Annual Cyber Security Report (latest).

- Limited forensic infrastructure
- Uneven capacity across states

Empirical data indicate a sharp rise in cybercrime cases but consistently low conviction rates, highlighting systemic inefficiencies.

EMERGING TRENDS AND TECHNOLOGICAL DEVELOPMENTS IN CYBERCRIME (2024–2026)

The period between 2024 and 2026 marks a significant turning point in the evolution of cybercrime, characterised by the convergence of advanced technologies such as artificial intelligence (AI), cloud computing, blockchain, and the Internet of Things (IoT)[12]. These developments have transformed cybercrime from isolated technical intrusions into complex, multi-layered socio-technical phenomena that challenge traditional legal and enforcement frameworks.

AI-Driven Cybercrime and Automation of Offences: One of the most transformative developments is the rise of AI-enabled cybercrime. Artificial intelligence has enabled cybercriminals to automate large-scale attacks, significantly increasing both efficiency and impact. Techniques such as:

- AI-powered phishing (hyper-personalised emails and messages)[13]
- Voice cloning scams using synthetic audio
- Deepfake video impersonation for financial fraud
- Automated malware generation

have made cybercrime more scalable and difficult to detect. Unlike traditional phishing, which relied on generic messaging, AI-driven attacks can analyse user behaviour and generate highly personalised content, increasing success rates. This shift represents a movement from volume-based cybercrime to precision-targeted attacks**,** requiring new forms of detection and legal recognition.

Deepfakes and Synthetic Identity Fraud: Deepfake technology has emerged as a major threat to both financial security and democratic processes. Cybercriminals now use AI-generated

[12] Europol, Internet Organised Crime Threat Assessment (latest).
[13] Europol, Internet Organised Crime Threat Assessment (latest).

images, videos, and audio to impersonate individuals, including corporate executives, government officials, and public figures.[14] Recent trends indicate a sharp increase in:

- Business Email Compromise (BEC) using deepfake audio/video
- Fraudulent investment schemes promoted through synthetic endorsements
- Identity theft through AI-generated biometric data

The legal challenge lies in attribution and authenticity. Existing evidentiary frameworks are not fully equipped to distinguish between genuine and manipulated digital content, raising questions about admissibility and burden of proof.

Furthermore, deepfakes blur the boundary between cybercrime and misinformation, creating hybrid offences that affect both economic and social stability.

"Digital Arrest" and Social Engineering Evolution: A particularly alarming development in India is the rise of so-called **"digital arrest scams."** In these schemes, cybercriminals impersonate law enforcement officials or regulatory authorities and coerce victims into transferring funds under the threat of arrest or legal action. These scams demonstrate a shift in cybercrime strategy:

- From technical exploitation → psychological manipulation
- From system vulnerabilities → human vulnerabilities

The success of such scams highlights deficiencies in public awareness, digital literacy, and verification mechanisms. Legally, these offences often fall under multiple provisions (fraud, impersonation, extortion), creating overlaps that complicate prosecution.

Cloud Computing and Jurisdictional Fragmentation: The increasing reliance on cloud infrastructure has significantly altered the nature of data storage and access. Data is now distributed across multiple jurisdictions, often managed by multinational corporations.

This creates several challenges:

- Unclear data location (multi-server distribution)
- Jurisdictional conflicts over access rights
- Dependence on foreign service providers

[14] World Economic Forum, Global Risks Report (latest).

- Delays in evidence retrieval

Cloud-based systems have effectively de-territorialised digital evidence**,** making traditional jurisdictional principles less effective. This reinforces the need for international cooperation mechanisms and standardised data access protocols.

Cryptocurrency and Financial Cybercrime: The rise of cryptocurrencies has introduced new dimensions to cybercrime, particularly in financial fraud, ransomware payments, and money laundering. Cryptocurrencies offer:[15]

- Anonymity or pseudo-anonymity
- Decentralised transaction systems
- Cross-border fund transfer without intermediaries

Cybercriminals increasingly use crypto assets to obscure financial trails, making investigation and asset recovery more difficult. While India has introduced regulatory oversight through taxation and reporting requirements, a comprehensive legal framework governing crypto-related cybercrime remains underdeveloped.

Internet of Things (IoT) and Expanding Attack Surfaces: The proliferation of IoT devices—including smart home systems, healthcare devices, and industrial sensors—has significantly expanded the cyber-attack surface. These devices often suffer from:

- Weak security protocols
- Lack of regular updates
- Poor encryption standards

As a result, they are frequently exploited in:

- Botnet attacks
- Distributed Denial of Service (DDoS) attacks
- Critical infrastructure breaches

The legal system currently lacks specific provisions addressing liability for IoT-related vulnerabilities, creating a regulatory gap.

[15] Jonathan Clough, Principles of Cybercrime (2nd edn, CUP 2015).

AI vs. Cybersecurity: The Technological Arms Race: A defining feature of modern cybercrime is the emergence of a **technological arms race** between attackers and defenders. While cybercriminals leverage AI to enhance attack sophistication, cybersecurity systems are also adopting AI for:

- Threat detection
- Behavioural analysis
- Automated response systems

However, this creates new challenges:

- Adversarial AI attacks**,** where attackers manipulate AI systems
- Data poisoning**,** compromising machine learning models
- False positives and bias in automated detection systems

This dynamic underscores the need for AI-aware legal frameworks capable of addressing both offensive and defensive uses of technology.

Socio-Legal Implications of Emerging Cybercrime: The evolution of cybercrime has broader socio-legal implications:

- Erosion of trust in digital systems
- Increased vulnerability of marginalised populations
- Blurring of boundaries between crime, misinformation, and national security threats

Cybercrime is no longer confined to economic loss; it increasingly affects **privacy, identity, and democratic processes**.

Synthesis: From Technical Crime to Socio-Technical Threat: The developments between 2024 and 2026 indicate a fundamental shift in cybercrime:[16]

Traditional Cybercrime	**Modern Cybercrime**
Technical intrusion	AI-driven manipulation

[16] Information Technology (Intermediary Guidelines) Rules 2026.

System-focused	Human + system focused.
Localized	Globally distributed
Reactive detection	Predictive and adaptive

This transformation highlights a critical challenge for India's legal system: existing laws are designed for static, technical offences, whereas modern cybercrime is dynamic, adaptive, and interdisciplinary.

To remain effective, cyber law must evolve beyond traditional criminal frameworks and incorporate technological, behavioural, and international dimensions.

Implications for India: For India, these trends underscore the urgency of reform in several areas:

- Development of AI-specific legal frameworks
- Integration of cybersecurity and criminal law
- Strengthening digital forensic capabilities
- Enhancing public awareness and cyber hygiene
- Building real-time international cooperation mechanisms

Without these reforms, the gap between cybercriminal capabilities and enforcement capacity will continue to widen.

RECENT LEGAL AND POLICY DEVELOPMENTS: A CRITICAL ANALYSIS (2023–2026)

India's cyber law and digital governance framework have undergone rapid transformation between 2023 and 2026, reflecting an attempt to respond to the exponential growth of cyber threats, artificial intelligence (AI), and data-driven economic systems. However, while these reforms signal strong legislative intent, their implementation reveals structural, procedural, and conceptual limitations.

Digital Personal Data Protection Act, 2023 and Rules, 2025: From Law to Implementation Gap: The Digital Personal Data Protection Act, 2023 represents India's first comprehensive data protection legislation, establishing a consent-based framework for data processing, user rights, and fiduciary accountability. Its operationalisation through the Digital Personal Data Protection Rules, 2025, introduces a fully digital Data Protection Board, enabling online complaint filing, adjudication, and appeals through electronic platforms.

The Rules also impose obligations such as consent-based data processing, data minimisation, breach reporting, and enhanced compliance requirements for "Significant Data Fiduciaries." However, emerging industry assessments indicate that a large number of organisations remain underprepared for compliance, highlighting a gap between legislative ambition and practical readiness.

Further, while the DPDP framework strengthens data governance, it does not fully address emerging risks such as AI-generated identity fraud, deepfake misuse, and synthetic data manipulation, thereby leaving critical gaps in regulating modern cyber threats.

IT Rules Amendment, 2026: The Shift Toward Platform Accountability: The amendment to the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules in 2026 marks a decisive shift toward proactive platform regulation. These changes impose stricter obligations on intermediaries, including mandatory labelling of AI-generated content, significantly reduced takedown timelines, and enhanced due diligence requirements.

This shift reflects a move from passive intermediary liability toward active responsibility for monitoring and controlling digital content. However, the aggressive enforcement timelines raise concerns regarding feasibility, potential over-censorship, and the risk of undermining procedural safeguards and due process.

Regulation of AI and Deepfakes: Emerging but Fragmented Framework: India's regulatory approach to artificial intelligence remains in a transitional phase. The emerging AI governance guidelines adopt a balanced approach, aiming to promote innovation while addressing ethical and security concerns.

Recent regulatory efforts have begun to focus on deepfake technology, requiring platforms to identify and manage synthetic media. However, the framework remains fragmented, with no

comprehensive legislation addressing AI-specific harms, liability standards, or evidentiary challenges.

This regulatory gap is particularly significant given the increasing use of AI in cybercrime, including impersonation, automated fraud, and misinformation campaigns.

Rise of AI-Driven Cybercrime and Policy Response: The increasing prevalence of AI-enabled cybercrime has fundamentally altered the threat landscape. Techniques such as deepfake-based fraud, voice cloning, and automated phishing have made cybercrime more scalable and difficult to detect.

Emerging scams, including impersonation of law enforcement authorities and financial institutions, demonstrate the growing sophistication of cybercriminal strategies. These developments highlight a shift from purely technical attacks to socio-psychological manipulation, exploiting human trust and behavioral vulnerabilities.

Government responses have emphasised the need for stronger coordination between law enforcement agencies and digital platforms, as well as enhanced public awareness and reporting mechanisms.

International Developments: UN Cybercrime Convention (2025): The United Nations Cybercrime Convention (2025) represents a significant effort to establish a global framework for cybercrime regulation. Unlike earlier agreements, it emphasises inclusivity, digital sovereignty, and privacy protections.

India's participation in this initiative reflects a growing willingness to engage in international cyber governance. However, concerns remain regarding the effectiveness of the Convention's operational mechanisms, particularly in enabling rapid cross-border cooperation.

Institutional and Governance Developments: Recent policy developments have also focused on strengthening institutional frameworks. These include the expansion of CERT-In's role, increased operational capacity of the Indian Cyber Crime Coordination Centre (I4C), and the introduction of digital reporting and grievance redressal mechanisms.

Despite these improvements, institutional fragmentation continues to hinder effective enforcement. Overlapping mandates, lack of coordination, and uneven capacity across states remain significant challenges.

Synthesis: The Emerging Direction of Indian Cyber Law: India's cyber governance framework is transitioning toward a more proactive and integrated model, combining elements of data protection, platform regulation, and AI governance. However, this transition remains incomplete.

The current system reflects a hybrid approach—legally progressive but operationally constrained. While regulatory frameworks are expanding, enforcement mechanisms have not evolved at the same pace.

The future effectiveness of India's cyber law regime will depend on its ability to integrate emerging technologies into legal frameworks, strengthen institutional coordination, and enhance international cooperation. Without these developments, the gap between legal authority and enforcement reality is likely to persist.

COMPARATIVE ANALYSIS

A comparative evaluation of cybercrime frameworks across major jurisdictions reveals that the effectiveness of cybercrime regulation depends not merely on statutory provisions but on the integration of legal, institutional, and technological systems. While India possesses a broad legislative framework, its operational limitations become more evident when contrasted with more coordinated global models.

European Union: Regulatory Integration and Preventive Governance: The European Union is the most sophisticated system of integrated cyber governance. Its structure unites data security, platform responsibility, and criminal control into a united regulatory ecosystem. General Data Protection Regulation (GDPR)[17] provides stringent requirements in data processing, which involve breach notifications, accountability, and severe financial fines in case of failure to comply. The Digital Services Act (DSA), which further extended platform liability to large online intermediaries, has seen this as a more recent development, as it requires large online intermediaries to actively discover, evaluate, and eliminate systemic risks, including disinformation, illegal content and cyber-enabled fraud.

There are three strengths of the EU model:

[17] Regulation (EU) 2016/679 (GDPR).

First, harmonisation of regulations throughout the member states, which minimises the jurisdictional differences. Second, good institutional coordination with institutions like Europol and Eurojust, which allows real-time investigations across borders. Third, preventive governance, implying the adoption of legal requirements in advance of the harm, other than resorting to post-crime prosecution.

Nevertheless, the EU approach is not free. Its strict compliance conditions are expensive to businesses, and its implementation in member states is spread differently. However, the EU proves that cybercrime regulation is best achieved when combined with larger digital governance frameworks.

United States: Decentralised but Operationally Efficient Model: The United States adopts a decentralised yet highly functional approach to cybercrime regulation. Its legal framework is distributed across multiple federal statutes, including the Computer Fraud and Abuse Act (CFAA), the Electronic Communications Privacy Act (ECPA), and sector-specific laws such as HIPAA and GLBA.

The distinguishing feature of the U.S. model is institutional capacity and **coordination**. Agencies such as the Federal Bureau of Investigation (FBI), Cybersecurity and Infrastructure Security Agency (CISA), and Department of Homeland Security (DHS) operate in a coordinated manner, supported by advanced technical infrastructure.

A key strength of this model is the emphasis on public-private partnerships. Information-sharing mechanisms between government agencies and private corporations enable real-time threat detection and response. Additionally, legislative tools such as the CLOUD Act [18]facilitate faster cross-border data access, addressing delays associated with traditional MLAT processes.

However, the U.S. framework faces criticism for fragmentation and privacy concerns. The absence of a unified data protection law creates inconsistencies, and expansive surveillance powers raise constitutional debates. Despite these issues, the operational efficiency of the U.S. system highlights the importance of capacity-building and technological integration.

Singapore: Centralised and Proactive Cyber Governance: Singapore is an example of centralised and very proactive cyber governance. The Cybersecurity Act, 2018, provides an

[18] Clarifying Lawful Overseas Use of Data Act 2018 (US).

all-encompassing regulatory model in regard to critical information infrastructure protection, incident reporting and compliance with security standards.[19]

The centralised institutional structure is the primary strength of the approach used by Singapore. The Cyber Security Agency (CSA) is a one-stop body that coordinates, enforces and provides policy change. This will do away with jurisdiction overlay and provide a quick response to cyberattacks.

Singapore also focuses on the future-oriented regulation that includes the use of AI-based threat detection, obligatory audits, and hard compliance requirements. Cross-border cooperation is also boosted by its cooperation with regional structures like ASEAN.

The main weakness of this model is that it is based on a comparatively smaller and tightly controlled digital ecosystem, which cannot be easily duplicated in a diverse and federal organisation such as India. It, however, proves the usefulness of centralised administration and quick-response systems.

China: Sovereignty-Driven Cyber Regulation: China adopts a state-centric approach to cyber governance, emphasising digital sovereignty and strict regulatory control. Laws such as the Cybersecurity Law (2017) and Data Security Law (2021) impose stringent data localisation requirements and grant extensive powers to the state.

The strength of this model lies in its strong enforcement capability and centralised authority, enabling rapid action against cyber threats. However, it raises significant concerns regarding privacy, state surveillance, and restrictions on cross-border data flows.[20]

While India shares certain concerns regarding data sovereignty, it has not adopted similarly stringent controls. The Chinese model highlights the trade-off between **security and civil liberties**, which remains a key consideration in cyber law policy.

India in Comparative Perspective: Structural Strength, Operational Weakness: India's cybercrime framework, when viewed comparatively, reflects a paradox. On one hand, it incorporates many advanced legal principles, including extraterritorial jurisdiction, data

[19] Cybersecurity Act 2018 (Singapore).
[20] Cybersecurity Law of the People's Republic of China 2017.

protection, and digital evidence recognition. On the other hand, it lacks the institutional coherence and procedural efficiency seen in other jurisdictions.

The key weaknesses of the Indian model include:

- Fragmented institutional structure, with overlapping responsibilities across multiple agencies
- Slow cross-border cooperation mechanisms, heavily dependent on MLAT processes
- Rigid evidentiary requirements, particularly in relation to digital authentication
- Limited public-private collaboration, reducing real-time threat intelligence sharing
- Uneven enforcement capacity, particularly between urban and rural regions

At the same time, India demonstrates certain strengths:

- A comprehensive statutory framework covering a wide range of cyber offences
- Increasing emphasis on data protection and digital governance through recent legislation
- Growing recognition of emerging threats such as AI-driven cybercrime

Comparative Synthesis: Key Insights: A cross-jurisdictional analysis reveals several critical insights:

1. **Integration is more important than legislation:** Jurisdictions with coordinated legal and institutional systems outperform those with fragmented frameworks.
2. **Speed is critical in cyber enforcement:** Real-time data sharing and rapid response mechanisms are essential.
3. **Preventive regulation is more effective than reactive enforcement:** Proactive obligations on platforms and organisations reduce cyber risks.
4. **Technological capacity determines enforcement success:** Investment in cyber forensics, AI tools, and digital infrastructure is crucial.
5. **International cooperation is indispensable:** Cybercrime cannot be addressed through domestic law alone.

Implications for India: For India, the comparative analysis highlights the need for a shift from a law-centric approach to a systems-based approach. Legal reforms must be accompanied by institutional integration, technological investment, and international engagement.

India's challenge is not the absence of legal authority but the inability to operationalise it effectively. Bridging this gap requires adopting elements from global best practices while adapting them to India's federal and socio-economic context.

Ultimately, the effectiveness of India's cybercrime framework will depend on its ability to transition from fragmented regulation to a coordinated, technology-driven governance model

JUDICIAL INTERPRETATION AND THE EVOLVING CYBER JURISPRUDENCE IN INDIA

The Indian judiciary has played a crucial role in shaping cyber law, particularly in interpreting jurisdictional principles, intermediary liability, and the admissibility of digital evidence. In the absence of fully developed statutory clarity—especially in emerging areas such as artificial intelligence (AI), deepfakes, and cross-border cybercrime—courts have increasingly adopted adaptive and pragmatic approaches to address the evolving nature of digital offences.

From Territoriality to Effects-Based Jurisdiction: One of the most significant contributions of Indian courts has been the gradual shift from strict territorial jurisdiction to a more flexible effects-based approach. In cases such as Yahoo! Inc. v. Akash Arora and SMC Pneumatics v. Jogesh Kwatra,[21] Courts recognised that cyber offences cannot be confined to physical boundaries and that jurisdiction may be determined by the location where harm occurs.

This approach has gained further relevance in contemporary cybercrime scenarios, where offences often involve cross-border data flows and decentralised digital infrastructures. The judiciary's willingness to prioritise impact over origin reflects an important doctrinal evolution aligned with global trends.

Constitutional Safeguards and Digital Rights: In Shreya Singhal v. Union of India,[22] the Supreme Court emphasised the importance of safeguarding freedom of speech in the digital sphere by striking down Section 66A of the IT Act. This case established a critical precedent that cyber regulation must operate within constitutional limits.

[21] Yahoo! Inc v Akash Arora 1999 PTC 201 (Del).
[22] Shreya Singhal v Union of India (2015) 5 SCC 1.

More recently, judicial reasoning has increasingly been influenced by privacy jurisprudence following K.S. Puttaswamy v. Union of India,[23] which recognised the right to privacy as a fundamental right. This has had significant implications for cybercrime investigations, particularly in balancing **state surveillance powers with individual rights**.

Digital Evidence and the Persistence of Procedural Rigidity: The landmark judgment in Anvar P.V. v. P.K. Basheer established strict requirements for the admissibility of electronic evidence, particularly through certification under evidentiary law. While this decision enhanced evidentiary integrity, it also created procedural bottlenecks—especially in cases involving cross-border data.

Despite the introduction of the Bharatiya Sakshya Adhiniyam, 2023, courts continue to grapple with challenges in authenticating digital evidence sourced from foreign jurisdictions or cloud-based systems. This has resulted in a tension between **legal formalism and technological practicality**, often weakening prosecution outcomes.

Judicial Response to Emerging Cybercrime Forms: The recent tendencies of the judicial sphere signify the growing interest in new types of cybercrime, especially those that may be related to deepfakes, impersonation, and massive financial fraud.

The courts have started to pass quick interim injunctions in lawsuits dealing with synthetic media and internet impersonation because of the irrevocable damage such content can cause. Nevertheless, the lack of statutory clarity regarding deepfakes and AI-generated materials constrains the uniformity of judicial reactions.

The emergence of so-called digital arrest scams has additionally revealed the loopholes in the interpretation of the law. These frauds include pretending to be law enforcement officials by calling in the video and falsifying legal papers by playing on the fear of prosecution by the victims. The recent incidents have shown that it is possible to put victims under long-term virtual custody and pressure them to give away large amounts of money.

As an example, in 2026, numerous cases in India were those in which victims were defrauded by such means, where people lost lakhs of rupees and were threatened with being falsely accused of crimes.

[23] K S Puttaswamy v Union of India (2017) 10 SCC 1.

According to judicial commentary and legal scholarship, such scams indicate that there is a more underlying problem, namely the absence of a certified digital state presence. The fraudsters can passably impersonate the processes of law enforcement since the citizens do not have a straightforward means of confirming the authenticity of digital communications.

Cybercrime Prosecution and Enforcement Reality: Current prosecutions point to the inability as well as the potential of the Indian system of enforcing cybercrime. High-profile cases, which have involved cyber fraud networks such as international fraud and online impersonation scams, show growing investigative capabilities. Yet, they also demonstrate that there are still long-standing issues with the possibility of tracing cross-border networks and obtaining digital evidence.

To illustrate, the current examples of fraud with the use of fake investment services, love scams, and the use of impersonation schemes demonstrate how cybercrime works across borders and takes advantage of the digital platform and social engineering.

Judicial proceedings in such cases often face delays due to:

- Difficulty in obtaining foreign evidence
- Complex financial tracing mechanisms
- Lack of standardised digital forensic protocols

AI, Deepfakes, and the Future of Judicial Interpretation: The emergence of AI-driven cybercrime presents new challenges for judicial interpretation. Deepfake technology, in particular, raises critical questions regarding:

- Authenticity of evidence
- Attribution of liability
- Burden of proof in synthetic media cases

Reports indicate a sharp increase in AI-enabled cyber fraud targeting Indian users, with large-scale scam networks leveraging social media platforms and automated tools. ()

Courts are increasingly required to evaluate not only the legality of actions but also the technical reliability of digital content**,** necessitating greater judicial familiarity with technological concepts.

Structural Limitations of Judicial Intervention: While the judiciary has demonstrated adaptability, its role remains inherently reactive. Courts can interpret and expand legal principles, but they cannot substitute for:

- Legislative clarity
- Institutional capacity
- Technological infrastructure

As cybercrime becomes faster, more decentralised, and technologically complex, the limitations of case-by-case adjudication become more evident.

Synthesis: Toward a Functional Cyber Jurisprudence: The evolution of cyber jurisprudence in India reflects a gradual transition from rigid territorial frameworks to more flexible, impact-based approaches. However, this evolution remains incomplete.

The key trends emerging from judicial interpretation include:

- Increasing reliance on effects-based jurisdiction
- Recognition of digital rights and privacy concerns
- Struggles with evidentiary modernisation
- Emerging engagement with AI-driven cyber threats

Ultimately, the judiciary has laid the foundation for a modern cyber law framework, but its effectiveness depends on parallel developments in legislation, institutional capacity, and technological integration.

Without such alignment, judicial innovation alone will be insufficient to bridge the gap between legal authority and enforcement reality.

KEY CHALLENGES IN INDIA'S CYBERCRIME FRAMEWORK

India's cybercrime regime, despite its expanding legal and policy framework, faces several structural and operational challenges that limit its effectiveness.

Jurisdictional Ambiguity: Cybercrime often spans multiple jurisdictions, creating uncertainty over investigative authority. Although Indian law provides for extraterritorial jurisdiction, its enforcement remains dependent on foreign cooperation, which is frequently slow and inconsistent.

Inefficient Cross-Border Cooperation: Mechanisms such as Mutual Legal Assistance Treaties (MLATs) are time-consuming and bureaucratic. Given the volatile nature of digital evidence, delays in international data sharing often result in loss of critical information.

Evidentiary Constraints: Despite reforms under the Bharatiya Sakshya Adhiniyam, challenges persist in the authentication and admissibility of digital evidence, particularly when sourced from foreign jurisdictions or cloud-based systems.

Institutional Fragmentation: Multiple agencies—including CERT-In, I4C, and state cyber cells—operate with overlapping mandates but limited coordination. This results in inefficiencies, duplication of efforts, and inconsistent enforcement.

Capacity and Infrastructure Gaps: Law enforcement agencies often lack advanced technical expertise, forensic tools, and trained personnel. These limitations are more pronounced in non-urban regions, leading to uneven enforcement capabilities.

Rise of AI-Driven and Social Engineering Attacks: Emerging threats such as deepfake fraud, voice cloning, and "digital arrest" scams exploit human psychology rather than technical vulnerabilities. Existing legal frameworks are not fully equipped to address these evolving forms of cybercrime.

Underreporting and Low Cyber Awareness: A significant proportion of cybercrime remains unreported due to a lack of awareness, limited trust in enforcement mechanisms, and social stigma. This undermines both data accuracy and policy response.

Gap Between Legal Framework and Enforcement: The most critical challenge is the disconnect between India's comprehensive legal framework and its limited enforcement capacity. While laws assert broad jurisdiction and regulatory control, practical implementation remains constrained by procedural delays, technological limitations, and coordination failures.

RECOMMENDATIONS: TOWARD AN EFFECTIVE AND ADAPTIVE CYBERCRIME FRAMEWORK

A multi-layer approach to solving cybercrime in India should include more than the expansion of legislation. The subsequent recommendations are geared towards closing the disjunction

between authority and capability of enforcement of the law through integration of legal, institutional, technological and international aspects.[24]

Legislative Harmonisation and Clarity: India's cybercrime laws currently operate through overlapping provisions under the Information Technology Act, the Bharatiya Nyaya Sanhita, and related statutes. This creates ambiguity in prosecution and enforcement.

- Consolidate cyber-related offences into **a** coherent and unified legal framework
- Clearly define emerging offences such as deepfake fraud, synthetic identity theft, and AI-assisted cybercrime
- Reduce overlap between general criminal law and specialised cyber legislation to ensure consistent application

Modernisation of Digital Evidence Framework: The effectiveness of cybercrime prosecution depends heavily on the admissibility and reliability of digital evidence.

- Introduce flexible evidentiary standards for electronic records, particularly in cross-border contexts
- Adopt technology-based verification methods, such as hash authentication and blockchain-backed chain-of-custody systems
- Align evidentiary rules with international best practices to facilitate cross-border admissibility

Strengthening Institutional Coordination: Institutional fragmentation remains a major obstacle to effective enforcement.

- Establish a centralised national cybercrime authority to coordinate between CERT-In, I4C, state cyber cells, and investigative agencies
- Develop standard operating procedures (SOPs) for inter-agency cooperation and case handling
- Implement real-time data-sharing platforms for coordinated investigation and response

Enhancing Law Enforcement Capacity: Cybercrime enforcement requires specialised technical expertise that is currently lacking in many regions.

- Invest in advanced cyber forensic infrastructure and AI-based investigation tools

[24] Chris Reed and John Angel, Computer Law (7th edn, OUP 2019).

- Introduce specialised training programs for police, prosecutors, and the judiciary
- Create dedicated cybercrime units and fast-track courts for handling complex digital cases

Regulating AI and Emerging Technologies: The rise of AI-driven cybercrime necessitates a dedicated regulatory approach.

- Develop a comprehensive AI regulatory framework addressing liability, accountability, and misuse
- Mandate traceability and labelling of AI-generated content, particularly in high-risk domains
- Establish clear legal standards for deepfakes, voice cloning, and synthetic media offences

Strengthening International Cooperation: Cybercrime is inherently transnational and cannot be addressed through domestic law alone.

- Negotiate bilateral and multilateral agreements for faster cross-border data sharing
- Streamline MLAT processes or adopt alternative fast-track cooperation mechanisms
- Consider strategic participation in global frameworks such as the UN Cybercrime Convention, while safeguarding national interests

Promoting Public-Private Partnerships: Given that much of the digital infrastructure is privately owned, collaboration with industry is essential.

- Establish formal information-sharing platforms between government agencies and technology companies
- Encourage joint cyber threat intelligence systems
- Incentivise private sector compliance through regulatory and financial mechanisms

Enhancing Cyber Awareness and Digital Literacy: A significant proportion of cybercrime exploits human vulnerabilities rather than technical flaws.

- Launch nationwide cyber awareness campaigns focusing on fraud prevention and reporting mechanisms
- Integrate cybersecurity education into school and university curricula
- Strengthen victim support systems to encourage reporting and reduce stigma

Improving Speed and Efficiency of Enforcement: The speed of cybercrime often exceeds the speed of legal processes.

- Introduce time-bound investigation and evidence collection protocols
- Enable real-time freezing of suspicious financial transactions
- Utilise automated monitoring systems **to** detect and respond to threats promptly

Adopting a Proactive and Technology-Driven Governance Model: India must move from reactive enforcement to proactive cyber governance.

- Implement predictive threat detection systems using AI and big data analytics
- Integrate cybersecurity, data protection, and criminal law into a unified digital governance framework
- Continuously update legal and policy frameworks to keep pace with technological advancements

CONCLUSION

The cybercrime system in India has high legal intent but low enforcement barriers. The main problem is not the lack of laws, but the inability of the laws to work. The development of threats like artificial intelligence-based fraud and deepfaking tricks continues to increase the disparity between legality and enforcement abilities. To solve this, there is a need to have a systemic shift in which legal change, technology and global cooperation are all involved. It is just such an approach that can help India to create a robust, efficient, and internationally oriented cyber justice system.