

CYBER CRIMES AND THE EVOLVING CRIMINAL LAW FRAMEWORK IN INDIA: FROM TECHNOLOGICAL OFFENCES TO THE PROBLEM OF DIGITAL ATTRIBUTION

Dr. Dharmender Kumar

¹Designation -Prof. & Dean (Faculty of Legal Studies), HRIT University, Ghaziabad (UP)

Received: 1st August, 2026; **Revised:** 5th August, 2026; **Accepted:** 8th August, 2026; **Available Online:** 20th August, 2026

ABSTRACT

The rapid expansion of digital technology has transformed the nature, scale, and geography of criminality in India. Cybercrime is no longer confined to conventional hacking or unauthorised access to computer systems. It now encompasses sophisticated forms of identity theft, financial fraud, ransomware, cyberstalking, online sexual exploitation, phishing, cryptocurrency-related offences, deepfake-enabled deception, artificial intelligence-assisted attacks, and coordinated disinformation. This transformation has placed considerable pressure on India's criminal justice system, which must simultaneously respond to technologically sophisticated offenders and preserve constitutional guarantees of privacy, liberty, due process, and fair trial.

This paper critically examines the evolution of India's criminal law framework in response to cybercrime. It analyses the interaction between the Information Technology Act, 2000, the Bharatiya Nyaya Sanhita, 2023, the Bharatiya Nagarik Suraksha Sanhita, 2023, and the Bharatiya Sakshya Adhiniyam, 2023. The paper argues that India's principal challenge is no longer the mere absence of laws against cybercrime. Rather, the central problem is what this paper conceptualises as the “**digital attribution gap**”—the increasing difficulty of connecting a digital act to a specific person, establishing criminal intent, preserving electronic evidence, and proving causation across anonymous, encrypted, transnational, and decentralised technological environments.

The paper proposes a new “**Five-A Model**” of **Cyber Criminal Justice**, consisting of Attribution, Authentication, Accountability, Adaptability, and Rights Protection. It argues that effective cybercrime regulation requires more than harsher punishment. India needs a coordinated framework that integrates technological investigation, cross-border cooperation, digital forensic capacity, evidence integrity, institutional accountability, and constitutional safeguards. The paper concludes that the future of Indian cybercrime law lies in moving from a **crime-centric model** to an **ecosystem-centric model**, where the law addresses not only the offender but also the digital infrastructure, platforms, intermediaries, financial systems, and institutional failures that enable cybercrime.

RESEARCH OBJECTIVES

The objectives of this research are:

1. To examine the evolution of cybercrime in India.
2. To analyse the statutory framework governing cyber offences.
3. To examine the relationship between cybercrime and traditional principles of criminal liability.
4. To identify the challenges of attribution and electronic evidence.
5. To analyse the constitutional implications of cybercrime investigation.
6. To propose a contemporary framework for cybercrime prevention, investigation, prosecution, and adjudication.

RESEARCH METHODOLOGY

A doctrinal and analytical methodology is used in this study.

The doctrinal component examines Indian legislation, constitutional principles, judicial decisions, and legal doctrines concerning cybercrime, electronic evidence, privacy, and criminal responsibility. The analytical component examines the changing technological environment in which cybercrime occurs.

The paper also adopts a conceptual approach by developing the theory of the **digital attribution gap** and proposing the **Five-A Model of Cyber Criminal Justice**. The research is primarily based upon secondary legal materials, including statutes, judicial decisions, academic literature, government publications, and policy documents.

Source of support: Nil.

Conflict of interest: Nil.

How to cite this article: Dharmender Kumar. CYBER CRIMES AND THE EVOLVING CRIMINAL LAW FRAMEWORK IN INDIA: FROM TECHNOLOGICAL OFFENCES TO THE PROBLEM OF DIGITAL ATTRIBUTION. Int J Drug Deliv Technol. 2026;16(84s):1530-1537. DOI: 10.25258/ijddt.16.84s.154.

INTRODUCTION

THE INFORMATION TECHNOLOGY ACT, 2000: THE FOUNDATION OF INDIAN CYBERCRIME LAW

The Information Technology Act, 2000 represents the foundation of India's statutory response to

cybercrime¹. The Act was introduced during an era when the internet was still developing and digital commerce was expanding². Its importance extends beyond cybercrime.

It also provided legal recognition to:

- electronic records;
- electronic signatures;
- digital transactions;
- electronic governance³.

The law's significance in combating illegal activity involving computers and digital systems has grown over time⁴. However, the technological environment has evolved dramatically since 2000. Modern cybercrime involves technologies that were either unknown or commercially insignificant when the legislation was enacted⁵. These include:

- cloud computing;
- encrypted messaging;
- cryptocurrencies;
- artificial intelligence;
- generative AI;
- deepfakes;
- autonomous systems;
- decentralised networks⁶.

The challenge is therefore not simply that the IT Act is old. The deeper problem is that **technology evolves faster than criminal law can be amended**. This leads to what is known as the "criminal law lag." Criminal law generally operates through relatively stable statutory categories. Technology, by contrast, evolves continuously. A legal provision may therefore remain formally valid while becoming practically inadequate to address new forms of criminal behaviour. The solution should not necessarily be to create a new offence every time a new technology appears. Instead, Indian cybercrime law should be drafted around technology-neutral principles of harm, deception, unauthorised access, interference, and exploitation.

THE BHARATIYA NYAYA SANHITA AND THE DIGITAL TRANSFORMATION OF CRIMINAL LAW

The enactment of the Bharatiya Nyaya Sanhita, 2023 represents a significant development in India's

substantive criminal law. Cybercrime, however, presents a unique challenge because many cyber offences operate at the intersection of specialised technology legislation and general criminal law. A cybercriminal may commit multiple offences simultaneously.

For example, a phishing operation may involve:

1. identity impersonation;
2. cheating;
3. unauthorised access;
4. financial fraud;
5. data theft.

This means that cybercrime should not be viewed exclusively through the IT Act. The BNS and other criminal statutes may also become relevant depending upon the facts of the case. The emerging model of Indian cybercrime law is therefore best understood as a **layered framework**:

Technology-specific offences

General criminal offences

Procedural investigation powers

Electronic evidence rules

Constitutional protections⁷

This layered structure is necessary because technology does not replace criminal conduct; it transforms the manner in which criminal conduct is committed.

THE DIGITAL ATTRIBUTION GAP

The most distinctive argument of this paper is that the central challenge in cybercrime prosecution is increasingly the problem of **digital attribution**. In conventional criminal law, attribution often depends upon physical evidence. In cybercrime, the situation is different⁸.

The evidence may consist of:

- IP addresses;
- device identifiers;
- login records;
- metadata;
- cloud records;
- blockchain transactions;
- encrypted communications;
- server logs;
- email headers⁹.

Yet none of these necessarily proves that a particular

Technology, Government of India, *India Cyber Threat Report 2023* (2023).

⁷ Information Technology Act, 2000; Bharatiya Nyaya Sanhita, 2023; Bharatiya Nagarik Suraksha Sanhita, 2023; Bharatiya Sakshya Adhiniyam, 2023; Constitution of India.

⁸ United Nations Office on Drugs and Crime, *Comprehensive Study on Cybercrime* (2013); Bharatiya Sakshya Adhiniyam, 2023.

⁹ Bharatiya Sakshya Adhiniyam, 2023; Information Technology Act, 2000; United Nations Office on Drugs and Crime, *Comprehensive Study on Cybercrime* (2013).

¹ Information Technology Act, 2000.

² Statement of Objects and Reasons, Information Technology Bill, 1999.

³ Information Technology Act, 2000, Section 4, 5, 6 and 10A.

⁴ Information Technology Act, 2000, ch. XI.

⁵ United Nations Office on Drugs and Crime, *Comprehensive Study on Cybercrime* (2013); Ministry of Electronics and Information Technology, Government of India, *India Cyber Threat Report 2023* (2023).

⁶ United Nations Office on Drugs and Crime, *Comprehensive Study on Cybercrime* (2013); Ministry of Electronics and Information

individual committed the crime. An IP address may identify a network rather than a person.

A device may be shared.

A digital account may be compromised.

A cryptocurrency wallet may be controlled through multiple individuals.

A person may be impersonated¹⁰.

The result is an important jurisprudential distinction:

Digital identity is not necessarily human identity.

This distinction should be central to cybercrime investigations.

The fact that an offence was committed through a particular digital account does not automatically establish that the account holder committed the offence. The prosecution must establish a sufficiently reliable connection between the digital activity and the accused¹¹. This is the digital attribution gap. It may be represented as:

Cyber Event → Digital Trace → Device → Account → Human Actor

The weakest point in many investigations is the final step. The law must bridge the gap between technological evidence and human responsibility.

THE PROBLEM OF ANONYMITY AND ENCRYPTION

Anonymity is one of the most significant challenges in cybercrime investigation. Criminal actors may use:

- VPNs;
- proxy servers;
- encrypted communication;
- anonymous accounts;
- temporary email addresses;
- cryptocurrency;
- dark-web infrastructure.

Encryption presents a particularly complex legal issue. On one hand, encryption protects legitimate privacy and cybersecurity. On the other hand, criminals may use encryption to conceal evidence. This creates a conflict between:

Privacy and security and Investigation and accountability

A democratic legal system cannot resolve this conflict simply by eliminating encryption. Weakening encryption for everyone may expose millions of ordinary citizens to greater cyber risk.

The better approach is targeted investigation based on lawful process. Cybercrime law should therefore aim to obtain relevant information through:

- judicially supervised warrants;
- lawful data requests;
- forensic analysis;
- international cooperation;
- targeted surveillance subject to constitutional safeguards.

The principle should be:

Investigative necessity must not become a justification for unlimited digital surveillance.

CYBERCRIME AND THE CHALLENGE OF MENS REA

Cybercrime also poses challenging issues related to criminal intent¹². Suppose a person clicks on a malicious link without knowing that it contains malware. Has that person committed a crime?¹³

Generally, criminal responsibility should depend upon the mental element required for the specific offence. Similarly, a cybersecurity researcher may access a system to identify vulnerabilities.

A hacker may access the same system to steal data.

The technical act may appear similar.

The intention is different¹⁴.

This demonstrates that cybercrime law cannot rely exclusively upon technical conduct. The law must distinguish between:

- authorised security testing;
- unauthorised access;
- criminal hacking;
- accidental access;
- malicious interference¹⁵.

The digital environment therefore reinforces the traditional importance of *mens rea*. Technology may automate an action, but criminal law must still determine the human intention behind it.

AI-ASSISTED CYBERCRIME

Artificial Intelligence is rapidly changing the cybercrime landscape¹⁶. AI may assist criminals in:

- creating highly convincing phishing messages;
- generating fake identities;
- automating social engineering;
- creating malicious code;

knowledge, intention or other prescribed mental element; see Bharatiya Nyaya Sanhita, 2023; Information Technology Act, 2000.

¹⁴ Information Technology Act, 2000, Section 43 and 66.

¹⁵ Information Technology Act, 2000, Section 43 and 66.

¹⁶ Ministry of Electronics and Information Technology, Government of India, *India Cyber Threat Report 2023* (2023); United Nations Office on Drugs and Crime, *Comprehensive Study on Cybercrime* (2013).

¹⁰ United Nations Office on Drugs and Crime, *Comprehensive Study on Cybercrime* (2013); see also Bharatiya Sakshya Adhiniyam, 2023.

¹¹ Bharatiya Sakshya Adhiniyam, 2023; *Anvar P.V. v. P.K. Basheer*, (2014) 10 SCC 473; *Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal*, (2020) 7 SCC 1.

¹² Bharatiya Nyaya Sanhita, 2023; Information Technology Act, 2000.

¹³ The criminal liability arising from such conduct would depend upon the ingredients of the specific offence, including any applicable requirement of

- conducting large-scale fraud;
- producing deepfake audio;
- impersonating public officials;
- manipulating financial communications¹⁷.

The significance of AI-assisted cybercrime lies in its ability to reduce the skill threshold required to commit sophisticated offences. The traditional cybercriminal needed technical expertise. AI may increasingly allow a person with limited technical knowledge to conduct complex attacks. This creates a new category of criminal conduct:

AI-amplified cybercrime.

The legal response should focus on the underlying criminal act. If a person knowingly uses AI to commit fraud, the existence of AI should not prevent prosecution¹⁸. However, a technology developer should not automatically become criminally liable merely because its general-purpose system was misused.

The law should examine:

- intent;
- knowledge;
- facilitation;
- foreseeability;
- control;
- contribution.

This is consistent with the concept of distributed culpability developed in contemporary AI criminal jurisprudence.

DEEPFAKES AND THE NEW ERA OF DIGITAL DECEPTION

Deepfakes represent a particularly serious development¹⁹. AI-generated audio and video can create apparently authentic representations of individuals saying or doing things that never occurred. This creates risks involving:

- financial fraud;
- political manipulation;
- defamation;
- sexual exploitation;
- blackmail;
- identity theft²⁰.

The criminal law problem is that digital evidence has traditionally been treated as valuable because it appears objective. Deepfakes challenge this assumption. The future question may not be: “Can digital evidence be produced?” It may instead be:

“**Can digital evidence be trusted?**” This creates a

new concept of **evidentiary insecurity**. The more sophisticated synthetic media becomes, the greater the need for:

- digital provenance;
- metadata verification;
- forensic authentication;
- chain-of-custody procedures;
- expert testimony²¹.

The criminal justice system must adapt before synthetic evidence becomes indistinguishable from authentic evidence.

ELECTRONIC EVIDENCE AND THE CRIMINAL TRIAL

Cybercrime prosecution depends heavily upon electronic evidence. However, electronic evidence presents several challenges. It may be:

- easily copied;
- altered;
- deleted;
- encrypted;
- stored outside India;
- distributed across multiple servers.

The Bharatiya Sakshya Adhiniyam, 2023 represents an important development in India's evidence framework. Nevertheless, legislation alone cannot guarantee evidentiary reliability. Investigators must maintain:

- proper chain of custody;
- forensic integrity;
- documentation;
- secure storage;
- authentication.

Courts must also distinguish between: **Digital evidence that establishes the occurrence of an event and Digital evidence that establishes the identity of the person responsible**. The two are not necessarily identical. For example, a digital transaction may establish that a fraudulent transfer occurred. It may not, by itself, establish who physically initiated the transaction. The prosecution must therefore establish the complete evidentiary chain.

CYBERCRIME AND THE RIGHT TO PRIVACY

The expansion of cybercrime investigation raises serious constitutional concerns. The Supreme Court's recognition of privacy as a fundamental right has transformed the constitutional framework within which digital investigation must operate. The State

¹⁷ Ministry of Electronics and Information Technology, Government of India, *India Cyber Threat Report 2023* (2023).

¹⁸ Bharatiya Nyaya Sanhita, 2023, provisions relating to cheating and fraud; Information Technology Act, 2000.

¹⁹ Ministry of Electronics and Information Technology, Government of India, *India Cyber Threat Report 2023* (2023).

²⁰ Bharatiya Nyaya Sanhita, 2023; Information Technology Act, 2000; Ministry of Electronics and Information Technology, Government of India, *India Cyber Threat Report 2023* (2023).

²¹ Bharatiya Sakshya Adhiniyam, 2023; *Anvar P.V. v. P.K. Basheer*, (2014) 10 SCC 473; *Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal*, (2020) 7 SCC 1.

may have legitimate reasons to investigate cybercrime.

However, investigative power must remain subject to constitutional limitations.

Digital devices contain extraordinary amounts of personal information. A smartphone may reveal:

- location;
- financial information;
- private communications;
- photographs;
- health information;
- personal relationships.

A search of a digital device may therefore be significantly more intrusive than a traditional physical search. This raises an important principle:

The constitutional significance of a search should depend not merely upon the physical object searched, but upon the informational depth of the search. Cybercrime investigation must therefore satisfy principles of legality, necessity, proportionality, and procedural safeguards.

CROSS-BORDER CYBERCRIME AND JURISDICTION

Cybercrime frequently crosses national borders.

An offender may operate from one country.

The victim may be located in another.

The server may be located in a third.

The financial institution may operate in a fourth.

This creates complex jurisdictional questions²².

Traditional criminal law is largely territorial.

Cybercrime is often geographically distributed.

This creates a fundamental mismatch: **Territorial law versus Borderless technology** international cooperation is therefore essential. India must strengthen cooperation through:

- mutual legal assistance;
- extradition mechanisms;
- information sharing;
- cross-border evidence preservation;
- coordinated cyber investigations²³.

However, international cooperation must also

respect privacy and due process. The objective should not simply be faster access to information. It should be **lawful, reliable, and accountable access to information**²⁴.

CYBERCRIME AND FINANCIAL FRAUD

One of the most rapidly expanding areas of cybercrime is digital financial fraud²⁵. The expansion of:

- mobile banking;
- digital wallets;
- instant payments;
- online lending;
- cryptocurrency;

has created new opportunities for criminals²⁶. Cybercriminals increasingly exploit human psychology rather than merely technological vulnerabilities. This is the rise of **social-engineering crime**. The criminal may not hack a bank. Instead, the criminal persuades the victim to voluntarily provide:

- passwords;
- OTPs;
- banking credentials;
- personal information²⁷.

This demonstrates that modern cybercrime operates at the intersection of:

technology + psychology + finance.

Criminal law must therefore be complemented by:

- financial monitoring;
- rapid freezing mechanisms;
- public awareness;
- platform accountability;
- cybersecurity education²⁸.

CYBERCRIME AGAINST WOMEN AND VULNERABLE GROUPS

Cybercrime has a disproportionate impact upon vulnerable individuals²⁹. Women may experience:

- cyberstalking;
- online harassment;
- image-based abuse;
- deepfake sexual content;

²² United Nations Office on Drugs and Crime, *Comprehensive Study on Cybercrime* (2013); Budapest Convention on Cybercrime, 2001.

²³ United Nations Office on Drugs and Crime, *Comprehensive Study on Cybercrime* (2013); Council of Europe, *Convention on Cybercrime* (Budapest Convention), 23 November 2001.

²⁴ Constitution of India, arts. 14 and 21; K.S. Puttaswamy (Retd.) v. Union of India, (2017) 10 SCC 1.

²⁵ Ministry of Home Affairs, Government of India, *Indian Cyber Crime Coordination Centre (I4C)*; Reserve Bank of India, relevant directions and advisories concerning digital payment fraud and cyber security.

²⁶ Reserve Bank of India, *Annual Report* (relevant year); Ministry of Home Affairs, Government of

India, *Indian Cyber Crime Coordination Centre (I4C)*.

²⁷ Reserve Bank of India, advisories concerning phishing, vishing, online banking fraud and protection of customer credentials.

²⁸ Reserve Bank of India, relevant directions and advisories concerning digital payment security and fraud prevention; Ministry of Home Affairs, Government of India, *Indian Cyber Crime Coordination Centre (I4C)*.

²⁹ United Nations Office on Drugs and Crime, *Comprehensive Study on Cybercrime* (2013); see also Information Technology Act, 2000; Bharatiya Nyaya Sanhita, 2023.

- identity impersonation;
- threats³⁰.

Children may face:

- online grooming;
- exploitation;
- cyberbullying;
- exposure to harmful content³¹.

The anonymity of cyberspace may encourage offenders who would otherwise be deterred in physical environments. This demonstrates that cybercrime is not merely a technological problem. It is also a problem of:

- gender justice;
- dignity;
- privacy;
- mental well-being;
- equality³².

The legal system must therefore adopt victim-sensitive procedures while ensuring effective investigation³³.

THE FIVE-A MODEL OF CYBER CRIMINAL JUSTICE

This paper proposes a new conceptual framework known as the **Five-A Model**.

A1: Attribution

The first objective is to identify the human actor responsible for the digital conduct. The law must bridge the gap between digital evidence and individual responsibility.

A2: Authentication

The second objective is to establish whether digital evidence is genuine. This is increasingly important in an age of deepfakes and AI-generated content³⁴.

A3: Accountability

The third objective is to determine responsibility across the entire cyber ecosystem. Responsibility may involve:

- offenders;
- accomplices;
- corporations;

- negligent institutions;
- platforms³⁵.

A4: Adaptability

Cybercrime law must evolve with technology. Rigid legislation may become obsolete. The law should therefore adopt technology-neutral principles capable of responding to future innovations.

A5: Rights Protection

The final objective is constitutional protection. Cybercrime investigation must not become an excuse for unlimited surveillance. Privacy, dignity, fair trial, and due process must remain central³⁶. The Five-A Model may therefore be represented as:

Attribution

↓

Authentication

↓

Accountability

↓

Adaptability

↓

Rights Protection

Together, these principles provide a framework for modern cyber-criminal justice.

THE PROBLEM OF PLATFORM ACCOUNTABILITY

Digital platforms occupy a complex position. They may be:

- communication intermediaries;
- social networks;
- financial platforms;
- content-hosting services³⁷.

Criminal actors may exploit these platforms³⁸. The question is whether platforms should be held criminally responsible for crimes committed by their users³⁹. Automatic liability would be inappropriate. Platforms cannot realistically prevent every criminal act⁴⁰. However, where a platform knowingly facilitates serious criminal activity, repeatedly ignores lawful requests, or deliberately designs systems to encourage harmful conduct,

³⁰ Bharatiya Nyaya Sanhita, 2023; Information Technology Act, 2000; Ministry of Home Affairs, Government of India, relevant cybercrime advisories.

³¹ Protection of Children from Sexual Offences Act, 2012; Information Technology Act, 2000; United Nations Office on Drugs and Crime, *Comprehensive Study on Cybercrime* (2013).

³² Constitution of India, arts. 14 and 21; K.S. Puttaswamy (Retd.) v. Union of India, (2017) 10 SCC 1.

³³ Bharatiya Nagarik Suraksha Sanhita, 2023; Bharatiya Nyaya Sanhita, 2023; Information Technology Act, 2000.

³⁴ Bharatiya Sakshya Adhiniyam, 2023; *Anvar P.V. v. P.K. Basheer*, (2014) 10 SCC 473; *Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal*, (2020) 7 SCC 1.

³⁵ Bharatiya Nyaya Sanhita, 2023; Information Technology Act, 2000; Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021.

³⁶ Constitution of India, arts. 14, 19 and 21; K.S. Puttaswamy (Retd.) v. Union of India, (2017) 10 SCC 1.

³⁷ Information Technology Act, 2000; Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021.

³⁸ United Nations Office on Drugs and Crime, *Comprehensive Study on Cybercrime* (2013); Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021.

³⁹ Information Technology Act, 2000, Section 79; Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021.

⁴⁰ Information Technology Act, 2000, Section 79.

accountability questions arise. The legal framework should therefore distinguish between: **Passive intermediary status and Active facilitation**. The difference may depend upon:

- knowledge;
- control;
- participation;
- financial benefit;
- failure to act after lawful notice⁴¹.

This approach avoids both excessive regulation and corporate immunity.

CYBERCRIME AND THE RIGHT TO FAIR TRIAL

The growth of cybercrime also affects criminal procedure.

Cybercrime cases may generate large volumes of digital evidence.

This creates a challenge for the defence.

If the prosecution produces thousands of pages of electronic records, logs, and technical reports, the accused must still receive a meaningful opportunity to challenge the evidence.

The right to a fair trial requires more than formal access to evidence.

It requires **effective access**.

The defence should have a meaningful opportunity to:

- examine digital evidence;
- challenge authenticity;
- question forensic experts;
- contest attribution;
- challenge algorithmic conclusions.

Technological complexity should not create a situation where the prosecution's evidence becomes effectively unchallengeable because it is too technical for ordinary legal scrutiny. This creates a new principle: **Digital complexity cannot be permitted to become a substitute for proof**.

CYBERCRIME INVESTIGATION AND THE DANGER OF OVERCRIMINALISATION

There is a growing tendency to respond to technological harm through criminalisation. However, not every digital wrong should become a criminal offence. Criminal law is the most coercive form of state power. It should therefore be reserved for conduct involving sufficient harm and culpability. A balanced framework should distinguish between:

- criminal conduct;
- civil wrongs;
- regulatory violations;
- platform policy violations;
- technological accidents.

Over-criminalisation may discourage cybersecurity research and technological innovation. A

cybersecurity professional testing a system with authorisation should not be treated identically to a criminal who intentionally exploits the same vulnerability. The law must therefore preserve the principle of **culpability-based criminalisation**.

RECOMMENDATIONS FOR REFORM

1. Develop a Comprehensive Cybercrime Policy

India should adopt a coordinated national framework integrating substantive criminal law, procedure, evidence, cybersecurity, and victim protection.

2. Strengthen Cyber Forensics

Every major investigative jurisdiction should have access to specialised digital forensic capacity.

3. Improve Police Training

Police officers should receive continuous training in:

- blockchain;
- cryptocurrency;
- AI;
- deepfakes;
- digital evidence;
- cyber forensics.

4. Create Specialised Cybercrime Courts

Complex cybercrime cases may require judges with specialised technological and evidentiary expertise.

5. Establish Digital Evidence Protocols

Uniform standards should govern:

- collection;
- preservation;
- authentication;
- storage;
- presentation.

6. Improve Cross-Border Cooperation

India should strengthen mechanisms for obtaining digital evidence located outside its territory.

7. Protect Encryption

Encryption should not be weakened indiscriminately. Investigative access should be targeted and legally supervised.

8. Establish Deepfake Detection Infrastructure

India should develop specialised systems for detecting synthetic media.

9. Strengthen Victim Compensation

Cybercrime victims, particularly victims of financial fraud and image-based abuse, require effective recovery and support mechanisms.

10. Promote Cybersecurity Education

Prevention must remain a central component of cybercrime policy.

CONCLUSION

Cybercrime has transformed the relationship between criminal law and technology. The central challenge facing India is not merely the creation of new cyber offences. The deeper challenge is the ability of the criminal justice system to identify,

⁴¹ Information Technology Act, 2000, Section 79; Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021.

prove, and attribute digital wrongdoing while preserving constitutional rights. The concept of the **digital attribution gap** provides a useful way to understand this problem.

A cybercrime may be visible.

The digital trace may exist.

The financial loss may be measurable.

Yet the human actor responsible may remain difficult to identify.

This gap between **digital occurrence** and **legal attribution** represents one of the greatest challenges for modern criminal jurisprudence. The response must therefore move beyond traditional crime-centric approaches. India requires an **ecosystem-centric model of cyber-criminal justice**. Such a model recognises that cybercrime occurs within a network involving:

Offenders

Digital platforms

Financial institutions

Technology providers

Investigative agencies

Courts

Victims

The proposed Five-A Model—**Attribution, Authentication, Accountability, Adaptability, and Rights Protection**—provides a framework for navigating this ecosystem. The future of Indian cybercrime law should therefore not be measured solely by the number of new offences created or the severity of punishment imposed. Its effectiveness should instead be measured by five questions:

Can the real offender be identified?

Can digital evidence be trusted?

Can responsibility be fairly attributed?

Can the law adapt to technological change?

Can constitutional rights survive the process?

The answer to these questions will determine whether India's criminal justice system can successfully transition from the age of physical crime to the age of digital criminality. The ultimate objective should be to create a legal system in which cyberspace is neither treated as a lawless zone nor subjected to unlimited state control. India must instead develop a model of **digital rule of law**—one in which technological innovation and criminal justice coexist under the principles of accountability, proportionality, evidence, and constitutional liberty.

REFERENCES AND SELECTED AUTHORITIES

Statutes

1. Constitution of India, 1950.
2. Information Technology Act, 2000.
3. Bharatiya Nyaya Sanhita, 2023.
4. Bharatiya Nagarik Suraksha Sanhita, 2023.
5. Bharatiya Sakshya Adhiniyam, 2023.

Judicial Authorities

1. *Shreya Singhal v. Union of India*, (2015) 5 SCC 1.

2. *K.S. Puttaswamy v. Union of India*, (2017) 10 SCC 1.
3. *Anvar P.V. v. P.K. Basheer*, (2014) 10 SCC 473.
4. *Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal*, (2020) 7 SCC 1.
5. *State of Tamil Nadu v. Suhas Katti*, C.C. No. 4680 of 2004.
6. *Sharat Babu Digumarti v. Government of NCT of Delhi*, (2017) 2 SCC 18.

Suggested Research Sources

1. Law Commission of India, reports concerning electronic evidence and criminal justice.
2. Ministry of Home Affairs, Government of India, publications relating to cybercrime.
3. Indian Computer Emergency Response Team (CERT-In), cybersecurity advisories and directions.
4. National Crime Records Bureau, *Crime in India* reports.
5. United Nations Office on Drugs and Crime, materials concerning cybercrime and electronic evidence.
6. Council of Europe, Budapest Convention-related materials concerning cybercrime cooperation.