Journal of Advances and Scholarly Research In Allied Education
Vol.23, Issue No.4 July 2026, ISSN 2230-7540

Cybercrime Governance in the Digital Age: Contemporary Challenges, Legal Responses and the Need for Reform in India

Lohit Kumar Bimal[1]*, Dr. Mani Kumar Meena[2]

[1] Research Scholar, Jaipur School of law, Maharaj Vinayak Global University, Jaipur, Rajasthan, India

lohitbimal23@gmail.com

[2] Supervisor, Jaipur School of law, Maharaj Vinayak Global University, Jaipur, Rajasthan, India

Abstract: Cybercrime governance has become an essential component of contemporary public administration, national security, economic regulation and protection of fundamental rights. The digitisation of banking, commerce, government services, communication and critical infrastructure has transformed cybercrime from an isolated law-enforcement concern into a systemic governance issue. Contemporary threats include ransomware, financial cyber fraud, identity theft, digital-arrest scams, phishing, cyberstalking, data breaches, deepfakes, AI-enabled impersonation, malicious synthetic media and attacks upon critical information infrastructure. These offences operate across institutional and territorial boundaries, requiring coordination between government departments, police organisations, banks, telecommunications companies, technology intermediaries, cybersecurity agencies and international partners.

India has created a multi-layered cyber-governance architecture centred around the Information Technology Act, 2000, CERT-In, the National Critical Information Infrastructure Protection Centre, the Indian Cyber Crime Coordination Centre, State cybercrime units, intermediary regulations and sector-specific regulators. The Bharatiya Nyaya Sanhita, 2023, Digital Personal Data Protection Act, 2023 and Bharatiya Sakshya Adhiniyam, 2023 have broadened the legal environment surrounding digital offences and electronic evidence. The Digital Personal Data Protection Rules, 2025 and Information Technology Amendment Rules, 2026 dealing with synthetically generated information further reflect a transition towards regulation of data security and AI-enabled harms.

Despite these developments, India's cyber-governance framework remains institutionally fragmented and continuously challenged by transnational crime, jurisdictional conflicts, rapid technological change, limited investigative capacity, delayed electronic-evidence acquisition and tensions between cybersecurity, privacy and freedom of expression. This article analyses the historical development and contemporary structure of cybercrime governance in India, evaluates regulatory and enforcement challenges and examines international models including the Budapest Convention, United Nations Convention against Cybercrime, NIS2 Directive and NIST Cybersecurity Framework. It argues for an integrated, rights-based and technologically neutral governance model combining prevention, resilience, criminal enforcement, corporate accountability, rapid financial intervention, victim protection and international cooperation.

Keywords: Cybercrime Governance; Digital Governance; Cybersecurity; Cyber Law; Information Technology Act; Artificial Intelligence; Data Protection; Intermediary Liability; CERT-In; I4C; Critical Infrastructure; Cyber Resilience; Regulatory Reform

INTRODUCTION

The relationship between crime and technology has undergone a fundamental transformation. Digital technology is no longer an independent sector operating alongside the conventional economy; it has become infrastructure through which modern society itself functions. Banking transactions, commercial contracts, healthcare records, educational systems, transportation, public administration and interpersonal communication increasingly depend upon networked technologies.

Consequently, cybercrime governance cannot be conceptualised merely as police action against hackers. It concerns the allocation of responsibility among States, corporations, technology platforms, financial institutions and users for preventing, detecting, investigating and responding to digitally mediated harm.

Governance is broader than legislation. A country may possess criminal offences prohibiting hacking, identity theft or online fraud yet remain vulnerable if banks cannot freeze suspicious transactions rapidly, platforms cannot preserve evidence, police lack forensic expertise, citizens cannot recognise social-engineering scams or critical infrastructure operators do not maintain effective incident-response procedures.

India's recent experience illustrates this distinction. NCRB data show that cybercrime registrations increased from 50,035 cases in 2020 to 52,974 in 2021, 65,893 in 2022, 86,420 in 2023 and **101,928 in 2024**. The growth reflects not only greater Internet use but increasing criminal exploitation of digital payments, communication platforms, identity information and social engineering.

The national reporting ecosystem records an even larger volume of victimisation. From 2021 to 2025, more than 6.58 million financial-fraud complaints were reported to the national system, involving reported losses exceeding ₹55,050 crore. By June 2026, more than ₹11,158 crore had reportedly been prevented from reaching fraudsters through the Citizen Financial Cyber Fraud Reporting and Management System.

These numbers reveal two important governance challenges. First, policing must operate at a scale substantially larger than traditional station-based crime reporting. Second, a successful

response frequently depends upon intervention within minutes or hours rather than the months or years associated with conventional criminal trials.

Financial cybercrime provides an obvious example. If a victim reports a fraudulent transfer immediately, banks and law-enforcement agencies may be able to identify receiving accounts and prevent further transfer. Once funds have passed through multiple mule accounts or virtual assets, recovery becomes significantly more difficult. Governance therefore begins before prosecution.

The same principle applies to cybersecurity incidents. A ransomware attack may be contained through effective backup, network segmentation and incident response. A data breach may be reduced through encryption and access controls. A deepfake may cause less harm if synthetic media can be quickly authenticated and labelled. Consequently, prevention and resilience must be recognised as components of justice policy.

India's cybercrime governance operates through multiple institutions. MeitY administers the Information Technology Act and significant aspects of intermediary and cybersecurity policy. CERT-In acts as the national cybersecurity incident-response agency. The National Critical Information Infrastructure Protection Centre performs specialised responsibilities concerning critical infrastructure. The Ministry of Home Affairs and I4C coordinate criminal-law responses and national cybercrime reporting. Police powers remain substantially exercised by States because police and public order fall within the State List. Financial regulators, telecommunications authorities and sector-specific agencies simultaneously perform relevant cybersecurity functions.

This distributed institutional architecture has advantages because cyber risk is sector-specific. However, fragmentation may produce overlapping mandates, inconsistent standards and uncertainty regarding responsibility.

The development of artificial intelligence illustrates the need for agile governance. AI enables economic innovation but can also create deepfakes, cloned voices and fabricated identities. India's February 2026 amendments to the IT Rules specifically responded to these risks by establishing due-diligence obligations relating to synthetically generated information.

Data protection creates another governance dimension. A leaked database containing names, mobile numbers, addresses and financial information may become the raw material for personalised fraud. Cybersecurity and privacy therefore overlap even though their legal objectives are not identical.

India's DPDP Rules, notified in November 2025, establish implementation standards concerning personal-data processing and security, but their commencement is phased. As of August 2026, not every substantive obligation within the rules has yet commenced. This transitional period makes organisational preparedness especially important.

The central thesis of this article is that the next generation of Indian cyber policy should move from **cybercrime law** towards **cybercrime governance**. This requires a coordinated framework incorporating security-by-design, corporate risk management, citizen awareness, rapid financial-fraud response, law-enforcement capability, data protection, intermediary accountability, international cooperation and constitutional safeguards.

Historical Background

The history of cybercrime governance reflects changing understandings of the relationship between information technology and public regulation. In the early period of computerisation, computers were largely confined to governments, universities, large corporations and specialised institutions. Computer misuse was therefore treated principally as an internal security or property problem. Unauthorised access might involve an employee manipulating records or an outsider entering a restricted system. Governance was predominantly organisational rather than societal.

The development of personal computing and interconnected networks during the 1980s gradually expanded both participation and vulnerability. States began adopting computer-misuse statutes because existing laws concerning theft, trespass and property damage did not clearly apply to intangible data. The conceptual difficulty was significant: an offender could copy confidential information without physically removing the original, or enter a computer system without entering a physical building.

The commercial expansion of the Internet during the 1990s fundamentally altered the governance problem. Electronic communications crossed national borders instantaneously.

Businesses began transferring value and information online. Criminal conduct therefore became simultaneously local in its effect and international in its technological execution.

International organisations recognised the need for legal harmonisation. The Council of Europe's Convention on Cybercrime, adopted in Budapest in 2001, became a major international instrument. It sought to harmonise substantive computer offences, establish procedural powers for electronic investigations and enable international cooperation. Its enduring importance lies partly in recognition that purely national approaches cannot adequately address transnational cybercrime.

India's first comprehensive cyber statute emerged within this international transformation. The Information Technology Act, 2000 provided legal recognition to electronic records and digital signatures and sought to facilitate electronic commerce and digital governance. Criminal and civil provisions concerning computer misuse were embedded within this larger commercial framework.

The statute represented a major legal innovation because Indian law had previously been constructed around paper documents, physical signatures and territorial conduct. Digital transactions required statutory recognition before courts, businesses and public authorities could confidently rely upon them.

Yet the Internet changed rapidly after 2000. Broadband connectivity, mobile devices, social networking, online banking and digital marketplaces generated new categories of risk. Phishing and identity fraud exposed limitations in the original Act. Communication platforms facilitated harassment, impersonation and unlawful dissemination of sexual material.

The Information Technology (Amendment) Act, 2008 therefore broadened the regulatory framework. Identity theft, cheating by personation using computer resources, violation of privacy and cyber terrorism were specifically addressed. Sections 70A and 70B strengthened the institutional foundations for protection of critical information infrastructure and cybersecurity incident response.

The amendment also developed the safe-harbour framework under Section 79, recognising that intermediaries should not automatically become criminally liable for every item of third-party content while requiring compliance with statutory conditions. This balance between

platform responsibility and intermediary immunity became one of the central issues of Indian Internet governance.

The constitutional limits of cyber regulation emerged prominently through ***Shreya Singhal v. Union of India***. Section 66-A had attempted to regulate certain electronic communications using vague expressions such as "grossly offensive" and "menacing." The Supreme Court held the section unconstitutional in 2015. The decision established an enduring principle: governmental concern regarding harmful online activity cannot justify vague criminal offences that disproportionately restrict lawful expression.

The Supreme Court's recognition of privacy as a fundamental right in ***Puttaswamy*** in 2017 further transformed digital governance. Cybersecurity measures can require collection of logs, identification information and communication metadata, while crime investigation may involve interception and surveillance. Such measures must operate within constitutional principles of legality, legitimate purpose, proportionality and procedural protection.

Institutional cybersecurity developed alongside jurisprudence. CERT-In became the national agency for incident response, advisories and cybersecurity coordination. NCIIPC developed specialised responsibility for critical information infrastructure. Sectoral regulators increasingly imposed security standards within banking, securities, telecommunications and other regulated sectors.

The Government's National Cyber Security Policy of 2013 attempted to provide an overarching framework concerning protection of information infrastructure, workforce development, incident response and public-private cooperation. Yet technological change soon accelerated beyond the policy assumptions of the period.

The introduction of UPI and rapid digital-payment adoption represented another transformation. Cybercrime increasingly shifted from attacks upon computers as objects towards attacks upon individuals through technology. Social engineering became central. Fraudsters did not necessarily need to defeat encryption if they could persuade a user to disclose an OTP, install remote-access software or approve a fraudulent transaction.

This transformation motivated new governance mechanisms. The Ministry of Home Affairs established the Indian Cyber Crime Coordination Centre to strengthen coordination among

law-enforcement agencies. The National Cyber Crime Reporting Portal created a central reporting interface, while the Citizen Financial Cyber Fraud Reporting and Management System introduced rapid coordination with financial institutions.

Government data show the scale of this approach. By June 2026, CFCFRMS had reportedly saved more than ₹11,158 crore across more than 32.80 lakh complaints. This represents a shift from reactive prosecution towards real-time harm prevention.

The IT Rules, 2021 expanded intermediary due-diligence and grievance-redressal requirements. Their evolution demonstrates a governance model in which private platforms exercise responsibilities that affect public safety, speech, privacy and criminal investigations.

Cybersecurity regulation became more prescriptive through CERT-In's April 2022 directions. Specified cybersecurity incidents must ordinarily be reported within six hours, and relevant entities are subject to requirements involving records and logs. The policy reflects recognition that national cybersecurity intelligence depends upon timely reporting by private and public organisations.

India's data-governance landscape underwent significant change through the DPDP Act, 2023. The Act establishes rights and obligations concerning digital personal data, while the DPDP Rules 2025 provide implementation details. The staged commencement recognises that organisations require transition time for compliance. Rules relating to major operational obligations are scheduled across different phases rather than taking effect simultaneously.

The introduction of the BNS and BSA from July 2024 created another stage. Traditional crimes such as cheating, personation, extortion and forgery increasingly occur through electronic means, and their prosecution must operate alongside technology-specific IT Act provisions.

By 2025–2026, AI-generated content became a central governance concern. The Government amended intermediary regulations to address synthetically generated information. MeitY identified deepfakes, identity fraud, misinformation, non-consensual imagery, reputational injury and extortion as relevant harms. The resulting 2026 rules require additional due diligence and synthetic-content identification.

The historical development therefore reveals a broader institutional transition. Cyber governance has moved through four overlapping stages: legal recognition of electronic transactions; criminalisation of computer misuse; institutional cybersecurity and platform accountability; and contemporary governance of data, AI, systemic resilience and financial cybercrime. India's challenge is now to integrate these layers coherently.

Conceptualising Cybercrime Governance

Cybercrime governance can be understood as the system of laws, institutions, technical standards, public policies and private-sector responsibilities through which digital crime risks are managed.

A narrow criminal-law model asks whether an act is prohibited and what punishment follows. A governance model asks additional questions: Could the attack have been prevented? Which organisation had responsibility to detect it? How quickly must it be reported? Who can preserve evidence? Who can freeze stolen funds? How should victims be compensated? What safeguards protect privacy and freedom of expression?

This broader approach recognises that cybercrime frequently arises from failures across an ecosystem.

For example, an identity-fraud operation may involve personal information obtained from a breach, a fraudulent SIM card, a spoofed call, a mule bank account and a social-media advertisement. No single regulator sees the entire chain. Effective governance therefore requires interoperability among agencies.

Contemporary Institutional Architecture in India

Ministry of Electronics and Information Technology

MeitY occupies a central position in India's digital regulatory framework. It administers the Information Technology Act and rules governing intermediaries and plays an important role in data-protection implementation and cybersecurity policy.

Its responsibilities place it at the intersection of innovation, platform regulation, security and individual rights.

CERT-In

CERT-In performs national incident-response responsibilities under Section 70B of the IT Act. It issues cybersecurity alerts and advisories, coordinates incident response and receives mandatory incident reports. The six-hour incident-reporting framework illustrates an important governance principle: significant cyber incidents are not merely private organisational matters because information concerning attacks can assist national threat detection.

National Critical Information Infrastructure Protection Centre

NCIIPC operates under Section 70A and focuses upon critical systems whose disruption could seriously affect national security, economy, public health or safety. Critical-infrastructure governance must increasingly consider supply-chain attacks, cloud dependencies, operational technology and third-party software risk.

Ministry of Home Affairs and I4C

Cybercrime investigation principally remains a policing matter, making MHA and State law-enforcement agencies central to the criminal-justice response. I4C provides national coordination and technological support. Government information released in 2026 identifies several important initiatives: the Samanvaya platform, Pratibimb analytics, Joint Cyber Coordination Teams, CyTrain, cyber forensic facilities and the Sahyog portal.

Samanvaya is particularly relevant because cybercriminal networks frequently operate across State boundaries. Analytics can identify repeated bank accounts, mobile numbers, devices or crime infrastructure appearing in complaints from different jurisdictions.

State Police and Cyber Police Stations

Because police and public order remain State subjects, effective cybercrime governance ultimately depends heavily upon State capacity. National platforms cannot substitute for well-trained investigators at district and police-station level.

This creates a federal challenge. Technological capabilities and staffing can vary substantially across jurisdictions. National standards, shared training and forensic support are therefore essential.

Financial Institutions

Banks, payment intermediaries and digital-payment systems are effectively frontline cybercrime institutions because financial fraud succeeds or fails partly through the speed with which funds can be transferred, frozen and restored. Anti-fraud monitoring should therefore be treated as a component of national cyber governance.

Telecom Operators

Fraudsters frequently exploit SIM cards, spoofed caller identities, bulk messaging and telecommunications infrastructure. Coordination between telecom operators, the Department of Telecommunications and law enforcement is therefore essential.

Technology Intermediaries

Social-media platforms, messaging services, hosting companies and online marketplaces possess data and technical capabilities relevant to cybercrime prevention and investigation. Section 79 of the IT Act and the IT Rules establish conditional safe harbour and due-diligence responsibilities. The challenge is to impose proportionate duties without transforming platforms into unaccountable private censors.

Artificial Intelligence and Synthetic Media Governance

Generative AI presents one of the most significant contemporary challenges because it simultaneously enhances legitimate productivity and lowers the cost of deception.

Voice-cloning technology can imitate family members or corporate executives. Deepfake videos can falsely depict public officials or private individuals. Synthetic sexual images can be used for harassment and extortion.

India's 2026 amendments specifically define synthetically generated information as relevant realistic synthetic audiovisual material and impose additional obligations. The framework

includes reasonable technical measures, labelling and provenance requirements and enhanced responsibilities for significant social-media intermediaries.

This development represents movement from content removal after harm towards authentication and provenance before harm.

Nevertheless, regulation must remain proportionate. AI tools used for accessibility, translation, ordinary editing, educational materials and legitimate creativity should not be treated as equivalent to malicious impersonation. MeitY's explanatory material expressly recognises several good-faith exclusions.

Data Governance and Cybercrime

Data breaches and cybercrime have a symbiotic relationship. Criminals frequently need information about victims before conducting personalised scams. Names, dates of birth, account details, addresses and transaction information can improve credibility.

The DPDP Act and Rules therefore indirectly contribute to crime prevention by requiring responsible personal-data processing and security safeguards. The 2025 Rules contemplate security measures including encryption, masking, access controls, logging, backup and technical and organisational safeguards. They also prescribe data-breach notification requirements when relevant provisions commence.

However, cybersecurity and privacy should not be conflated. An organisation can be cybersecurity-secure while still collecting excessive data, and it can respect data minimisation while maintaining inadequate technical security. Effective governance must address both.

Challenges in Cybercrime Governance

Institutional Fragmentation

Multiple agencies possess legitimate but overlapping responsibilities. MeitY, MHA, CERT-In, NCIIPC, State police, telecom authorities and financial regulators may all become involved in a single incident.

A serious ransomware attack on a bank, for example, may simultaneously involve cybersecurity reporting, criminal investigation, sectoral financial regulation, data breach notification and critical-infrastructure concerns. Without clearly defined escalation protocols, fragmentation can delay response.

Federal Coordination

Cybercrime rarely respects State boundaries. A victim in Rajasthan may transfer funds into an account in another State operated by a mule acting for a network located elsewhere. Traditional police jurisdiction was designed around geographical offences. Digital policing requires interoperable databases, rapid interstate requests and common procedures. The Joint Cyber Coordination Team model and Samanvaya platform are therefore important developments.

Cross-Border Evidence

Global platforms may store relevant information outside India. Criminal infrastructure may operate from foreign servers. Conventional mutual legal assistance can be too slow for volatile digital evidence. India's future treaty strategy should therefore prioritise electronic-evidence access while preserving sovereignty, privacy and due process.

Attribution

Digital identity does not automatically correspond to legal identity. A device, SIM card or account may be stolen, compromised or operated by a mule. Law must avoid over-reliance on technological identifiers. Attribution should involve corroborated forensic, financial and contextual evidence.

Corporate Under-Reporting

Organisations may hesitate to disclose cyber incidents because of reputational and commercial concerns. Mandatory reporting can improve national awareness, but excessive or duplicative requirements can generate compliance fatigue. India should continue rationalising reporting obligations across CERT-In, data-protection authorities and sectoral regulators.

Digital Literacy

A sophisticated cybersecurity system cannot completely prevent a user from voluntarily transferring money to a criminal after being deceived. Public awareness must therefore address human vulnerabilities. Citizens should understand that legitimate law-enforcement agencies do not conduct *"digital arrests"* through video calls or require transfers to *"safe accounts."*

Victim-Centred Governance

Traditional criminal justice concentrates upon investigation and punishment. Cybercrime requires equal emphasis upon stopping loss and restoring funds. The development of the Money Restoration Module and grievance mechanisms within CFCFRMS reflects a more victim-oriented approach. Future policy should measure success partly by restitution rates, not merely arrests.

Privacy, Surveillance and Constitutional Balance

Cybercrime governance inevitably creates tension between security and privacy. Investigators may require subscriber information, communication metadata, device contents and financial records. Governments may seek data retention and interception capabilities. However, cybersecurity should not become an unrestricted justification for surveillance.

The right to privacy recognised in *Puttaswamy* requires intrusions to satisfy constitutional standards. Likewise, *Shreya Singhal* demonstrates that harmful online conduct cannot justify vague restrictions upon expression. A rights-based governance model requires legality, necessity, proportionality, oversight and effective remedies.

Encryption presents a particularly difficult issue. Strong encryption protects banking, commerce, government communication and personal privacy. The same encryption may be used by criminals. Weakening encryption generally may create systemic vulnerabilities greater than the investigative benefit obtained. Policy should therefore favour targeted investigative methods over universal weakening of security architecture.

Regulatory Reforms Required in India

A Comprehensive Cyber-Law Review

The IT Act remains foundational but was enacted more than a quarter-century ago. Incremental amendments have created a layered framework that may be difficult to navigate. India should consider comprehensive statutory modernisation while preserving constitutional jurisprudence and settled principles that remain effective.

Technology-Neutral Offence Definitions

Laws should criminalise harmful conduct rather than particular technologies wherever possible. A statutory provision tied too closely to today's platform may become obsolete tomorrow.

Unified Cyber-Incident Governance

Organisations frequently face different reporting requirements under cybersecurity, financial and data-protection frameworks. A coordinated reporting gateway could reduce duplication while distributing information to competent agencies according to statutory authority.

Specialised Cybercrime Courts or Judicial Capacity

Cybercrime litigation frequently involves technical evidence. Whether through designated courts or specialised judicial training, decision-makers should understand digital forensics, blockchain tracing and electronic-evidence preservation.

Enhanced Corporate Responsibility

Cybersecurity governance should become a board-level responsibility in high-risk organisations. Management should maintain incident-response plans, test backup procedures and conduct supply-chain risk assessments. The EU's NIS2 model illustrates how regulatory duties can extend beyond technical departments towards governance accountability.

National Cybercrime Victim Framework

India should consider a structured victim-assistance framework covering rapid fraud reporting, financial restoration, counselling for severe cyber harassment, identity remediation and legal assistance.

Regulation of Mule Accounts

Banks should employ behavioural analytics and enhanced monitoring to identify accounts showing unusual rapid inflows and dispersals. However, account-freezing powers must include safeguards for innocent persons whose accounts may have unknowingly received tainted transfers.

AI Authentication Standards

Synthetic-content regulation should evolve towards interoperable provenance standards, cryptographic authenticity and visible labelling. Regulation should focus upon deceptive or harmful uses rather than suppressing AI technology itself.

Continuous Capacity Building

Cyber training cannot be a one-time qualification. Investigators, prosecutors and judges require continuous updating because offender methods evolve faster than traditional training cycles.

International Perspectives

Budapest Convention

The Budapest Convention remains an influential framework for cybercrime legislation and international electronic-evidence cooperation. Its substantive provisions address illegal access, system interference, computer-related fraud and other offences, while procedural provisions facilitate investigation and preservation of electronic evidence. India has not historically joined the Convention. Concerns regarding sovereignty and cross-border data access influenced this position. Nevertheless, the Convention's procedural mechanisms remain relevant comparative material.

United Nations Convention Against Cybercrime

The adoption of the UN Convention against Cybercrime in December 2024 constitutes a major development because it provides a genuinely global negotiating framework. The Convention seeks international cooperation concerning cyber-dependent crimes and electronic evidence for serious offences. As of August 2026, it had 81 signatories and three parties and had not yet entered into force. India should carefully evaluate participation and implementation because a global treaty could significantly affect future electronic-evidence cooperation.

European Union

The EU has increasingly adopted a systemic risk-governance model. The NIS2 Directive requires essential and important entities to adopt cybersecurity risk-management measures covering incident handling, business continuity, supply chains, vulnerability management, cryptography and employee training. The value of NIS2 lies in shifting attention from post-crime prosecution to organisational resilience.

United States

The American model combines federal criminal legislation, sector-specific regulation, law-enforcement institutions and voluntary technical standards. NIST's Cybersecurity Framework 2.0 introduces six functions: Govern, Identify, Protect, Detect, Respond and Recover. The explicit inclusion of governance reflects recognition that cybersecurity is fundamentally an organisational leadership responsibility.

Lessons for India

International comparison suggests five broad lessons. First, harmonised definitions facilitate cooperation. Second, electronic-evidence mechanisms must operate rapidly. Third, critical-sector resilience requires affirmative governance duties. Fourth, cybersecurity should involve executive-level accountability. Fifth, international cooperation must coexist with human-rights safeguards. India should adapt these principles to its constitutional and federal structure rather than mechanically transplant foreign laws.

CONCLUSION

Cybercrime governance has become indispensable to India's digital future. The increase in registered cases to more than one lakh in 2024 demonstrates that technological expansion is accompanied by substantial criminal risk.

India has already developed a sophisticated network of laws and institutions. The Information Technology Act, CERT-In, NCIIPC, I4C, the National Cyber Crime Reporting Portal, DPDP framework, BNS and evolving intermediary regulations provide substantial foundations. The next stage should focus on integration. Cybersecurity, criminal law, financial regulation, data protection and intermediary governance should not operate as isolated silos.

A governance-based approach recognises that the best cybercrime case may be the one prevented before money is lost or data compromised. Rapid intervention, resilient infrastructure, secure data practices and informed citizens are therefore as important as prosecution. At the same time, security must remain constitutionally constrained. Privacy, expression, encryption and procedural fairness cannot be sacrificed in pursuit of a perfectly monitored digital environment.

The appropriate objective is neither unrestricted cyberspace nor unrestricted State control. It is a trustworthy digital ecosystem in which innovation, security, accountability and fundamental rights reinforce rather than undermine each other.

FUTURE SCOPE

Future cybercrime-governance research should develop empirical measures of institutional effectiveness. The number of complaints or arrests alone cannot determine whether governance mechanisms work. Research should examine the time taken to freeze fraudulent transactions, proportion of funds restored, investigation duration and conviction outcomes.

Second, the emerging role of generative AI demands continuous study. Researchers should examine how synthetic identities, autonomous agents, voice cloning and deepfakes change offender behaviour and evidentiary standards.

Third, India requires greater academic analysis of cybercrime federalism. Comparative evaluation of State cyber police units may identify best practices that can be replicated nationally.

Fourth, the operational relationship between DPDP breach requirements and CERT-In incident reporting should be examined as phased DPDP obligations take effect.

Fifth, the emerging United Nations Convention against Cybercrime will create an important field of scholarship concerning sovereignty, electronic evidence, privacy and international cooperation.

Sixth, research should explore cybercrime victimology more deeply. Senior citizens, children, women, small businesses and first-time Internet users may face distinct risks requiring targeted interventions.

Seventh, future studies should consider cybercrime economics. Understanding money-mule networks, advertising infrastructure, hosting services and payment channels can identify points at which criminal ecosystems can be disrupted economically.

Finally, India's future cyber-governance model should increasingly incorporate multidisciplinary expertise. Lawyers alone cannot govern cyberspace, just as technologists alone cannot determine questions of liberty and justice. Effective policy requires lawyers, computer scientists, psychologists, economists, law-enforcement professionals, cybersecurity practitioners and civil-society organisations to work together.

References

1. Government of India. (2000). *The Information Technology Act, 2000*. Government of India.
2. Council of Europe. (2001). *Convention on Cybercrime*. Council of Europe.
3. Wall, D. S. (2007). *Cybercrime: The transformation of crime in the information age*. Polity Press.
4. Government of India. (2008). *Information Technology (Amendment) Act, 2008*. Government of India.
5. Brenner, S. W. (2010). *Cybercrime: Criminal threats from cyberspace*. Praeger.

6. Government of India. (2013). *National Cyber Security Policy 2013*. Department of Electronics and Information Technology.
7. *Shreya Singhal v. Union of India*, (2015) 5 SCC 1.
8. Clough, J. (2015). *Principles of cybercrime* (2nd ed.). Cambridge University Press.
9. *Justice K.S. Puttaswamy (Retd.) v. Union of India*, (2017) 10 SCC 1.
10. Holt, T. J., Bossler, A. M., & Seigfried-Spellar, K. C. (2018). *Cybercrime and digital forensics: An introduction* (2nd ed.). Routledge.
11. Government of India. (2021). *Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021*. Ministry of Electronics and Information Technology.
12. Indian Computer Emergency Response Team. (2022). *Directions under sub-section (6) of Section 70B of the Information Technology Act, 2000 relating to information security practices, procedure, prevention, response and reporting of cyber incidents*. CERT-In.
13. European Parliament & Council of the European Union. (2022). *Directive (EU) 2022/2555 concerning measures for a high common level of cybersecurity across the Union*. Official Journal of the European Union.
14. Government of India. (2023). *Digital Personal Data Protection Act, 2023*. Ministry of Law and Justice.
15. Government of India. (2023). *Bharatiya Nyaya Sanhita, 2023*. Ministry of Law and Justice.
16. Government of India. (2023). *Bharatiya Sakshya Adhiniyam, 2023*. Ministry of Law and Justice.
17. National Institute of Standards and Technology. (2024). *The NIST Cybersecurity Framework (CSF) 2.0*. U.S. Department of Commerce.
18. United Nations General Assembly. (2024). *United Nations Convention against Cybercrime: Strengthening international cooperation for combating certain crimes committed by means of information and communications technology systems and for the sharing of evidence in electronic form of serious crimes* (A/RES/79/243).
19. Government of India. (2025). *Digital Personal Data Protection Rules, 2025*. Ministry of Electronics and Information Technology.
20. Government of India. (2026). *Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Amendment Rules, 2026*. Ministry of Electronics and Information Technology.

21. National Crime Records Bureau. (2026). *Crime in India 2024*. Ministry of Home Affairs, Government of India.

22. Ministry of Home Affairs. (2026). *National cybercrime data*. Government of India.