



## MSB-International Journal of Interdisciplinary Research

Associating Researchers; Nourishing Innovation

Peer Reviewed

Vol. 3, Issue 1, March 2025-June 2025

54-68, MSB-IJIR

### Law of Cybercrime Legislation and Global Cooperation in India

Gitanshu Koushik <sup>1</sup>

Dr Juhi Sexena <sup>2</sup>

<sup>1</sup>LL.M, Amity Law School

<sup>2</sup>Assistant Professor, Amity Law School,  
Amity University, Lucknow, Uttar Pradesh

#### Abstract

*The rapid development of cyberspace and the increasing penetration of digital technology in everyday life have opened a new frontier of crime: cybercrime. As one of the largest digital economies in the world, India has unique challenges in keeping pace with the increasing threat from cybercrime perpetrators. The "Law of Cybercrime Legislation and Global Cooperation in India" explains the legal frameworks that regulate cybercrime in India, like the Information Technology Act, 2000, and its amendment. It also explores the mechanisms of global cooperation for cybercrime investigation with focus on how India engages with global cooperation to fight cross-border cybercrime. The article considers the strengths and weaknesses of India's domestic legislation and law enforcement body, as well as how they compare with international standards, and the need for increased international cooperation. Comparing the international role of India in cyber policy-making, international treaties, and capacity-building, the article concludes by stressing the need for bi-lateral and multi-lateral alliances to tackle cybercrime. The role of cyber diplomacy, policy initiatives, and emerging technological trends in shaping India's cybercrime legislation and international alliances is examined. The abstract seeks to gain some understanding of India's strategic positioning in the international world of cybercrime, its problems pertaining to legislation, and its ability to ensure stronger global alliances.*

**Keywords:** Cybercrime, Cybercrime Legislation, India, Global Cooperation, Information Technology Act, International Cooperation, Cybersecurity, Digital Economy, Law Enforcement, Cyber Diplomacy

## Introduction

The "Law of Cybercrime Legislation and International Cooperation in India" is an emerging critical area of legal scholarship and policy debate in the 21st century, particularly in the context of new cyber threats, digital dependency, and globalization. Since India is fast digitizing, placing technology in every nook and corner of governance, business, and life, the necessity for a robust and holistic legal framework to counter cybercrime has become paramount. Cybercrimes range from data theft, identity theft, and hacking to sophisticated cyber terrorism and cyber financial fraud. The Indian legal system has evolved significantly during the past decades to meet these new challenges, particularly through the enactment and amendment of the Information Technology Act, 2000, which forms the bedrock of Indian cyber law. But with the fast-changing dynamics of cyber attacks and the boundary-less character of cybercrime, domestic law alone is insufficient. It demands seamless global coordination, congruence between legal systems, and strategic collaborations between nations and international agencies. The Information Technology Act, 2000 (IT Act), and its several amendments form the basic legal framework to combat cybercrimes in India. Originally targeted at facilitating electronic commerce and legalizing electronic signatures, the Act was later revised, most prominently in 2008, to encompass a wider scope of cyber crimes like cyber terrorism, voyeurism, data theft, and identity theft. Despite these legal steps, enforcement remains problematic due to the inexistence of technical skills within traditional law enforcement agencies and the absence of a unified international legal framework. Additionally, there is a wide disparity between the pace at which technologies are advancing and how legislation has evolved, leading to many loopholes within law that are still being exploited by cybercriminals. Indian law regarding cybercrime is evolving slowly, as courts often resort to interpretation of outdated laws or international principles of law where there are no comprehensive domestic regulations. India's engagement with international cooperation schemes in the fight against cybercrimes becomes increasingly relevant with the contemporary digital economy. As cybercrimes are of an international character, they mainly set up shop beyond jurisdictions where Indian laws do not have a direct applicability. This necessitates high level of international cooperation towards investigation, sharing of information, extradition, and prosecution. India is a member of several multilateral forums and discussions such as the United Nations, INTERPOL, and the G20 Digital Economy Task Force, where cybersecurity and cybercrime are the priority agenda items. India is not a signatory to the Budapest Convention on Cybercrime, however, which is an international treaty that first tackled Internet and computer crime by harmonizing national law, improving investigation techniques, and improving cooperation between states. The non-membership in this convention, primarily because of sovereignty concerns and the absence of representation from developing countries in its formulation, has both diplomatic and pragmatic implications for India's international cooperation on cybercrime law. In a bid to align domestic law with

international enforcement frameworks, India has been actively developing bilateral and multilateral agreements with a group of nations.<sup>1</sup>

These treaties facilitate mutual legal cooperation, cyber threat intelligence sharing, and joint capacity-building programs for law enforcement agencies. India has signed cyber cooperation agreements with other countries like the United States, Russia, Australia, and members of the European Union, among others. These partnerships are necessary in order to obtain digital evidence located overseas and battle criminal networks exploiting jurisdictional boundaries for evading prosecution. Apart from that, India is also investing in enhancing its legal enforcement capacity through the creation of specialized cybercrime cells at the state level, cyber forensics training of personnel, and the encouragement of public-private partnerships to enhance cybersecurity resilience. The emergence of new technologies such as artificial intelligence, blockchain, and the Internet of Things (IoT) also presents new challenges that current cybercrime laws are not well equipped to deal with. The Indian judicial system needs to adapt in light of these technological developments by way of constant updating of legal terminology, techniques, and policing authority. Moreover, privacy concerns, as elucidated in the landmark Supreme Court judgment that recognized the right to privacy as a fundamental right under the Constitution of India, provide a further level of complexity to the legal landscape. Balancing cybersecurity surveillance and protection of individual rights is a highly sensitive but crucial task for legislators and enforcing agencies. For this reason, it is crucial that there be a multi-pronged approach encompassing legislative reform, international collaboration, institution building, and technological innovation to effectively counter cybercrime in India.<sup>2</sup>

### **Major Cybercrime Trends in India**

In the Indian context, cybercrime trends have seen a spectacular transformation over the last decade in terms of both complexity and volume. With the swift penetration of the internet and mobile technologies, India has become one of the world's largest digital user populations. This enormous digital expanse, however, has increasingly found itself exposed to a broad range of cyber threats. Some of the most prevalent cybercrime trends are financial scams, ransomware, phishing, cyberstalking, identity theft, and cyber defamation. With online financial services and electronic transactions becoming an integral part of daily life, cybercriminals have exploited loopholes in cybersecurity mechanisms, user ignorance, and relaxed regulatory enforcement to conduct sophisticated frauds. Unauthorised use of banking data, tampering with e-wallets, and UPI fraud transactions have increased exponentially, resulting in monetary loss as well as erosion of confidence in digital platforms. All this is compelling the Indian judicial system to transcend traditional notions of theft and fraud to adopt technologically advanced definitions and solutions. Phishing attacks, in particular, have emerged as an area of

---

1 Information Technology Act, 2000, No. 21, Acts of Parliament, 2000 (India), amended by Information Technology

(Amendment) Act, 2008, No. 10, Acts of Parliament, 2008 (India); United Nations, "Cybercrime," <https://www.un.org/en/cybercrime>.

2 Ministry of External Affairs, "Bilateral Cooperation in Cyber Security," (2022), <https://mea.gov.in>.

concern, targeting individuals and institutions. Cybercriminals use social engineering techniques to trick users into revealing sensitive data such as login credentials, credit card information, and personal identification data. These attacks have become more sophisticated with the use of AI-generated content and deepfake technologies, which complicate it for users to distinguish between real and simulated communications. These have been preceded by a notable surge in ransomware attacks against critical sectors such as healthcare, education, and public utilities. Malware used in such attacks encrypts data and requires payment of a ransom for its release, typically paid in untraceable cryptocurrency. Indian companies and government agencies have been among the primary targets due to presumed vulnerabilities in their cybersecurity frameworks and poorly prepared incident response processes. The Indian legal and regulatory infrastructure is thus under perpetual pressure to adapt and keep pace with such fast-moving forms of cybercrime. Another major trend in Indian cybercrime is the exploitation and victimization of women and children through online abuse, harassment, bullying, and exploitation. The access and anonymity provided by the internet have empowered perpetrators, resulting in an increase in cases of nonconsensual sharing of intimate images, impersonation, and cyberstalking. The offenses not only violate individual privacy but also cause societal harms because they reinforce a culture of fear and digital insecurity. While the Information Technology Act, 2000, does have provisions to address some of these offenses, enforcement is uneven, and victims do not report such crimes due to stigma, ignorance, or lack of confidence in the justice system. This has resulted in calls for more gender-sensitive cyber laws, police training, and the creation of safe reporting mechanisms that ensure victim protection and speedy justice. India has also witnessed a sharp increase in cyber espionage, cyber terrorism, and politically motivated cyber attacks.<sup>3</sup>

As geopolitical tensions at South Asia and at a global level, state-sponsored cyber operations have risen to the forefront. Critical infrastructure industries such as electric power grids, communication systems, defence systems, and governmental databases have become regular targets for cyber compromises and surveillance activities. These developments form the foundation of the growing convergence between national security and cybercrime that requires a cross-domain solution that integrates classical defence principles with cyber intelligence, diplomacy, and protection under law. The Indian legal structure, in collaboration with foreign partners, is more and more embracing developing end-to-end constructs to meet these advanced threats. But this is a difficult endeavour in that jurisdiction, varying levels of sectors' levels of cybersecurity maturity, and the nature of state-sponsored cyber operations are issues. Synergistic to these developments have been dark-web and cryptocurrency-related cybercrimes, which have also expanded, presenting new regulatory challenges to Indian regulators. The dark web is the hub of illicit transactions, ranging from drug smuggling, weapon sales, and sale of stolen information and attack mechanisms. Cryptocurrency, while a technological development of immense potential, has also become the preferred method of transaction for cybercriminals due to perceived anonymity and limited traceability. India's legislative and regulatory apparatus continue to struggle to cope with finding adequate ways

---

3 Press Information Bureau, "Cyber Security Incidents in Critical Infrastructure Sectors," (2023), <https://pib.gov.in>.

of controlling and monitoring such activity. Though the Reserve Bank of India (RBI) and draft legislation have made efforts to control the application of cryptocurrency, the absence of a clear-cut, uniform legal stance has provided room for a grey area to flourish, which cybercriminals readily exploit. This vagueness complicates law enforcement and requires an integrated policy action with the involvement of financial regulators, cybersecurity experts, and international allies.<sup>4</sup>

### **The Information Technology Act, 2000**

The Information Technology Act, 2000 is the pillar of Indian cybercrime law and the legal basis of India's efforts to regulate digital space, secure electronic transactions, and combat cyber crimes. Enacted at the dawn of the new millennium, the Act was a move by the Indian government to respond to the threat posed by an emerging digital economy and the simultaneous upsurge in cybercrimes. It was drafted in accordance with the United Nations Model Law on Electronic Commerce, designed to provide legal recognition to electronic records and digital signatures. As years went by and technology progressed and cyber attacks became sophisticated, the Act came to be widely amended, most notably in 2008, which extended its scope far beyond its original commercial purpose. These amendments incorporated significant provisions that sought to tackle a vast spectrum of cybercrimes, thereby propelling the IT Act from being a regulatory bill on online transactions to a cornerstone piece of India's cybersecurity and cybercrime management infrastructure. IT Act, in its revised form, addresses various classes of crimes ranging from unauthorized access and hacking to identity theft, cyberstalking, phishing, and cyberterrorism. It criminalizes a range of acts including tampering with computer source material, distributing obscene content in electronic form, and sending offensive messages through communications services. Section 66 itself deals with offenses relating to computers and has been further divided to address specific offenses like identity theft (Section 66C), cheating by impersonation through a computer resource (Section 66D), and cyber terrorism (Section 66F). These provisions of law mirror India's effort to stay in line with the evolving digital threat environment and to establish a legal framework capable of dealing with the intricacies of cybercrime. Nevertheless, in spite of the broad legislative mandate, problems related to enforcement, judicial interpretation, and public awareness continue to detract from the Act's overall effectiveness in combating cybercrime. One of the major aspects of the Information Technology Act is that it provides for adjudication of cyber disputes and establishing a legal mechanism to resolve them. The Act confers adjudicating officers and the Cyber Appellate Tribunal (which subsequently merged into the Telecom Disputes Settlement and Appellate Tribunal) jurisdiction to deal with cases pertaining to contraventions under the Act. While this was a significant step toward institutionalizing the enforcement of cyber law, working implementation issues have plagued the system. Delays in disposal of cases, inadequate technologically competent personnel, and jurisdiction issues have limited the effectiveness of the tribunal. Furthermore, since the interfacing between cybercrime and regular crime has increasingly become common, common courts have often been involved in interpreting and making rulings regarding cyber cases. This has resulted in variation in the

---

4 Justice K.S. Puttaswamy (Retd.) v. Union of India, (2017) 10 SCC 1 (India).

interpretation of the law and also the demand for uniform legal education and cyber forensic support across the judiciary. IT Act also provides for provisions regarding security and confidentiality of information.<sup>5</sup>

Section 43A, to give another instance, requires firms handling sensitive personal data to follow reasonable security practices and procedures and provides relief by way of compensation in case of negligence leading to breach of data. The provision has gained extreme significance after a string of high-profile data breaches and leaks in India's private as well as public space. However, the absence of a master law on data protection to support the IT Act has created a gap in regulation. Data privacy matters are therefore usually not addressed or addressed in an ad-hoc manner. There was a need for a robust regime of data protection, in supplement to the IT Act, since the Supreme Court's 2017 judgment recognizing the right of privacy as part of the essential rights under the Indian Constitution reinforced the need further. The court's judgment made expectations from the legal system high to adequately preserve privacy of citizens in the contemporary digital age. Again, one of the key features of the Information Technology Act is its emphasis on intermediary liability and obligations upon internet service providers, social networking websites, and online content hosts. Section 79 of the Act gives qualified immunity to intermediaries for third-party content, provided only that they follow due diligence standards and obey government or judicial orders for content takedown. This need has ignited heated debate regarding freedom of expression, censorship, and the role of technology platforms in regulating online content. As with the proliferation of false news, hate speech, and cyber extremism, the government has tried to tighten these norms by introducing legislation like the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021. The rules impose a greater burden on intermediaries to identify the "first originator" of a message, comply with data preservation requirements, and offer grievance redress mechanisms. While intended to deter abuse of online services, these legislations have also drawn criticism from international actors and civil society for posing the potential of deterring freedom of expression and anonymity of users.<sup>6</sup>

### **Law Enforcement and Judicial Mechanisms**

Judicial and law enforcement procedures are pivotal and dynamic in the enforcement and effectiveness of cybercrime laws in India, particularly in the broader perspective of international cooperation. The growing size and sophistication of cyber-attacks have necessitated a rethink and restructuring of traditional law enforcement strategies and judicial procedures. Indian police officials, who have long been used to dealing with conventional crimes, have had to adjust to keep up with the speed of cybercrimes that are often very technological, anonymized, and global in nature. The Indian government has therefore reacted to this by attempting to enhance its policing model through the establishment of specialized cybercrime cells, improving forensic capabilities, and investment in training programs that can improve digital literacy levels among police officers. All these efforts are critical in a

---

5 Justice K.S. Puttaswamy (Retd.) v. Union of India, (2017) 10 SCC 1 (India).

6 Carnegie India, "Intermediary Liability and Encryption: Policy Challenges in India," (2022), <https://carnegieindia.org>.

society where cybercriminals frequently exploit jurisdictional confusion and technological loopholes to operate with impunity. The National Investigation Agency (NIA) and the Central Bureau of Investigation (CBI), India's premier investigation agency, have also acquired a more active role in probing cybercrimes with a national security dimension or cross-border impact. The majority of police forces at the state level have also set up cybercrime cells that handle grievances related to cyber frauds, cyber stalking, hacking, and identity theft. But the capacity of these units varies widely from state to state, reflecting the uneven development of cyber infrastructure and expertise in the nation. Most of these cells do not have trained professionals, high-tech equipment, and connectivity to realtime digital evidence, which hinders the efficiency of the investigation. Second, due to the everchanging dynamics of cybercrime, there is always a delay in the understanding and implementation of relevant legal provisions, leading to underreporting and low rates of conviction. This situation calls for a systemic need for standard training procedures, centralized data-sharing infrastructure, and incorporation of cyber intelligence into broader policing policies. On the legal side, the Indian judiciary system has increasingly begun to grapple with the particular challenges posed by cybercrime by setting up specialist cybercrime courts and including modules on cybercrime in judicial courses.<sup>7</sup>

Judicial officers are increasingly required to bring themselves to work on complex technical evidence, read digital forensic reports, and translate international legal cooperation requests, each of which represents a significant deviation from traditional legal analysis. Evolution of the court's approach has found expression in its growing adoption of electronic evidence at criminal proceedings and its readiness to provide directions to the government bodies and technological companies regarding retention of information and management of content. Judicial processes, however, have traditionally grappled with procedural delays, case backlog, and a deficit of uniform jurisprudence with respect to issues relating to the cyber space. Such challenges are exacerbated when cyber-crimes cross several jurisdictions, which then need courts to depend on foreign assistance and treaties that are necessarily time-consuming and diplomatically volatile. The procedural machinery for adjudicating cybercrime cases has also had to adapt to the technicality of the offenses in the digital world. Collection, storage, and admissibility of electronic evidence is controlled by specific sections of the Indian Evidence Act, as the said Act is modified by the IT Act, 2000. Electronic evidence by nature is sensitive and easily manipulable and therefore the courts have made stern chain-of-custody guidelines and proof in accordance with Section 65B of the Evidence Act. Despite these provisions, many cases fail in court due to procedural failures, insufficient forensic examination, or mishandling of digital data. This illustrates the urgent need for institutional capacity building in digital forensics and the establishment of state-of-the-art forensic laboratories across the country. There are efforts to enhance these capabilities by establishing partnerships with

---

7 Internet Freedom Foundation, "Capacity Gaps in India's Cybercrime Law Enforcement," (2021), <https://internetfreedom.in>.

schools, private sector cybersecurity firms, and foreign organizations, but the pace and scale of change must be commensurate with the changing threat landscape.<sup>8</sup>

### **Capacity Building and Infrastructure Gaps**

Capacity development and the building of infrastructure are the vital pillars of India's struggle against cybercrime, more so with respect to consolidating the law of cybercrime legislation as well as building international cooperation. While India has achieved a lot legislatively in terms of enacting and amending the Information Technology Act, 2000, the effectiveness of any legal framework ultimately depends upon the readiness of the institutions that need to implement and enforce it. Unfortunately, it is here that some of the significant capacity and infrastructure gaps lie. Nationally, there remains a glaring imbalance between the technological, skilled human resources, and procedural expertise that are needed to fight cybercrime in an integrated and coordinated manner. The state and district police departments, especially, lack the sophisticated tools to confront advanced cyber attacks due to antiquated hardware, restricted access to forensic tools, and limited in-service training of police personnel. These handicaps create vulnerabilities for exploitation by cybercriminals, especially in rural and semi-urban areas where public as well as police levels of digitization are typically low. India's investigation and judicial apparatus also do not have the technical competence in cybercrime, which demands specialized training and infrastructure needs. The forensic laboratories, upon which the analysis of digital evidence depends, are few and overburdened with backlogs.<sup>9</sup> Few states have fully functional cyber forensic labs, and even if some do, they mostly don't have current software and equipment to examine encrypted data, blockchain ledgers, or dark web traffic. Forensic experts who are capable of addressing emerging technologies such as artificial intelligence, deepfakes, cryptocurrency, and cloud digital forensics are also in dire need. The lack of such expertise not only hinders investigations but also undermines the integrity of evidence presented in court, which in turn affects conviction rates. Even if digital evidence is recovered, it is hard to guarantee its admissibility in court due to procedural lapses, particularly those related to certification and preservation of electronic documents under applicable legal provisions. At the policy level, the Government of India realized the necessity for capacity development and has launched some initiatives aimed at institutional capacity building. One such initiative is the Indian Cyber Crime Coordination Centre (I4C), established as a platform providing coordinated cybercrime investigation, training, research, and development at the national level. The I4C is conceived to function as a capacity-building nodal center for the police through offering modules on cybercrime investigation, cyber forensics, and legal aspects of cyber crime. But implementation and extent of such efforts are uneven in different regions, and the decentralized nature of policing in India places yet another complicating factor over the search for standardization. State police forces operate with limited budgets and face bureaucratic hurdles in accessing central resources. Hence, the necessity for a successful

---

8 Digital Evidence and Cross-border Cooperation," (2023), <https://www.meity.gov.in>.

9 Report on Capacity Gaps in India's Cybercrime Ecosystem," (2021), <https://internetfreedom.in>.

federal-state partnership model for ensuring consistency in cybercrime response mechanisms with strong funding and institutional support is justified.<sup>10</sup>

### **Global Perspective on Cybercrime Laws**

The global awareness of cybercrime legislation is required to understand the broader context within which India's cybercrime legislation and cooperative effort must function. Cybercrime, by definition, is not geographically contained. It operates transnationally, involves actors in multiple countries, and exploits the differences between national legal frameworks. Here, the international community has made significant leaps towards harmonization of cyber legislation, facilitating cooperation across borders, and establishing unified standards for inquiry and prosecution. There have been several international agreements, conventions, and cooperative platforms that have been established in recent decades to shape a collective worldwide response to cyberspace challenges. These include the Council of Europe's Budapest Convention on Cybercrime, the United Nations' initiatives for combating cybercrime and electronic governance, and the OECD's privacy protection and transborder data flow policies. These instruments seek to converge definitions of cyber-crimes, impose legal obligations on member states, and promote cooperation in digital evidence exchange, capacity building, and technical cooperation. The Budapest Convention of 2001 remains the most extensive and best-supported international cybercrime treaty. It offers a legal tool for criminalizing many forms of online exploitation, such as unauthorized access, interference with data, interference with systems, and fraud affecting computers. Notably, it provides procedures for cooperation between countries, including expedited preservation of stored computer data, mutual legal assistance, and international investigation. Over 65 nations have ratified or acceded to the convention, including some from Asia, Africa, and Latin America. India, however, is surprisingly not a signatory to the Budapest Convention due to objections against its drafting process, which excluded most developing countries, and possible implications on sovereignty and domestic legal procedures. India has preferred to support a more universal, United Nations-brooked treaty on cybercrime that represents the Global South interests and assures equitable participation. India nevertheless treats signatory states with bilateral arrangements, which are typically slow and bureaucratic compared to multilateral treaty procedures under such an example as the Budapest Convention. The increasing intersectionality of cyber-diplomacy and international diplomacy has led states to add cybercrime issues on foreign policy and national security platforms.<sup>11</sup>

Cyber diplomacy has emerged as a tool to advance strategic interests, negotiate international norms, and create coalitions against cyber threats. The United States, United Kingdom, Australia, and the European Union members have adopted formal strategies that align cybersecurity with national defence, economic security, and human rights. These strategies are

---

10 National Judicial Academy, "Training Needs and Gaps in Digital Evidence Handling," (2022), <https://nja.gov.in>.

11 Internet Freedom Foundation, "India, Cyber Sovereignty, and Global Cybercrime Treaties," (2022), <https://internetfreedom.in>.

followed by extensive networks of cyber attaches, interagency coordination mechanisms, and multilateral working groups. On the other hand, while India has made considerable progress in embracing cybersecurity as a strategic necessity, its institutional mechanism for cyber diplomacy is still in the making. The Ministry of External Affairs has set up a New and Emerging Strategic Technologies Division to engage with global forums, but greater consistency in India's cyber foreign policy is required, particularly in aligning domestic legal norms with international expectations. A crucial aspect of the global perspective towards cybercrime legislation is how to balance security against personal rights. As governments around the world ramp up cyber controls to contain threats on the internet, fears have been voiced regarding the possibility of surveillance, censorship, and invasion of privacy. Democratic nations are under pressure to weigh balancing the authority to empower law enforcement agencies against the protection of civil liberties in the internet age. This battle can be witnessed in global discourse on data localization, intermediary liability, and end-to-end encryption. Countries like the United States and members of the European Union have enacted strong privacy laws such as the General Data Protection Regulation (GDPR) and thus lead the global discourse on consumer protection and data protection. India, although it does have provisions in the Information Technology Act for the protection of data, is developing a stronger legislative framework through its Digital Personal Data Protection Act. Nevertheless, India's surveillance law, secrecy over data access procedures, and recent regulatory guidelines to technology companies have been condemned as compromising privacy and free speech, exemplifying the fineness of meeting global standards while dealing with local requirements.

12

### **India's Role in Global Cybercrime Cooperation**

India's role in international cybercrime cooperation has grown significantly in the past two decades, keeping pace with its emergence as a major digital economy and rising power in global cyber governance. As cybercrime increasingly traverses borders to penetrate global financial markets, critical infrastructures, and national security, India has valued being an active participant in international regimes and alliances that facilitate greater cooperation to fight cyber threats. With one of the largest internet user populations and an expanding tech ecosystem, India is well positioned to influence global cyber norms, inform legal standards, and participate in cooperative law enforcement platforms. Its international cooperation on cybercrime is not unidimensional, involving bilateral treaties, membership of multilateral platforms, contributions to capacity building initiatives, and incremental harmonization of its domestic law with international standards. India has entered into numerous bilateral agreements and memoranda of understanding (MoUs) with countries like the United States, United Kingdom, Russia, France, Japan, and Australia, among others, in the realm of cybercrime investigation, exchange of digital evidence, and cyber forensics training. Bilateral agreements have facilitated the exchange of technical know-how and real-time threat intelligence, which is critical given the borderless nature of cybercrime. For example, India

---

12 Internet Freedom Foundation, "India's Surveillance Laws and Data Access Provisions: A Critical Analysis," (2023), <https://internetfreedom.in>.

and America have established working groups under their strategic partnership to address the issue of cybersecurity as well as critical infrastructure protection. These are extended to police agencies as well, where Indian officials collaborate closely with such bodies as the FBI, Europol, and INTERPOL to track and capture cybercrime that operates across jurisdictions. These alliances are vital in combating transnational cyber fraud-related offenses, child exploitation networks, ransomware operations, and state-sponsored cyber espionage. Multilaterally, India has been a dynamic participant in regional and international platforms that aim to enhance cooperation in cybersecurity and cybercrime regulation. India is a member of such forums as the G20 Digital Economy Task Force, the Shanghai Cooperation Organisation (SCO), the BRICS Working Group on ICT and High-Performance Computing, the ASEAN Regional Forum, and the Global Forum on Cyber Expertise. These forums are key forums for dialogue, establishing trust, and creating norms in cyberspace. India has been a sponsor of efforts within the United Nations to consolidate efforts towards a universal international treaty on cybercrime in the UN Ad Hoc Committee on Cybercrime. India has not signed the Budapest Convention because India is troubled by its Eurocentric background and limited inclusiveness, while India advocates for a UN initiative that considers the perspectives and legal cultures of developing nations. This corresponds to India's broader diplomatic approach towards digital sovereignty and balanced international governance of the Internet space.<sup>13</sup>

### **Cyber Diplomacy and Policy Initiatives**

Cyber diplomacy and policy initiatives have emerged as crucial components of India's broader strategy for countering the emerging threat of cybercrime while facilitating global cooperation and projecting its position in global digital governance. With rising digital interdependence between states, the scope of cyber diplomacy has expanded beyond security and technical interests to include economic interests, geopolitics, internet governance, and human rights. India, as a rising digital power with a huge cyber infrastructure and a growing technology-driven economy, has also felt the need to use diplomacy not only for the security of its cyberspace but also to shape the global cyber norms that govern cross-border data flows, digital trade, privacy practices, and cooperation in cybercrime. India's cyber diplomacy is predominantly conducted by the Ministry of External Affairs in the New and Emerging Strategic Technologies (NEST) department, which interacts with other national bodies such as the Ministry of Home Affairs, Ministry of Electronics and Information Technology (MeitY), and the National Security Council Secretariat. This intra-bureaucratic collaboration seeks to ensure India's foreign activities on cyber issues in conformity with its domestic policy interests, security needs, and technological ambitions. India's cyber diplomacy has focused on the institution of bilateral and multilateral cyber negotiations, participation in global cyber governance forums, promotion of responsible state behaviour in the cyber realm, and the advocacy of the balanced development of international digital assets. These efforts align with India's vision of strategic autonomy and digital sovereignty, which deal with the sovereignty

---

13 Press Information Bureau, "India's Stand on the Budapest Convention on Cybercrime and Support for a UN-Centered Approach," (2023), <https://pib.gov.in>.

of states in controlling their cyberspace in addition to internal laws and developmental needs.<sup>14</sup>

On the issue of bilateral interactions, India has engaged in well-enunciated cyber dialogues with other key powers of the world like the United States, European Union, Japan, United Kingdom, Australia, Russia, and Israel. These dialogues are mechanisms for the exchange of information on threats, coordination of cybercrime enforcement policies, best practices in terms of cybersecurity standards, and mechanisms for legal cooperation. They also facilitate mutual assistance in the investigation of cybercrime and have been instrumental in building confidence and technical interoperability between countries. Further, India has signed several memoranda of understanding in cyber cooperation and cybercrime that specifically aim at cooperation in the aspect of protection of critical information infrastructure, response to cyber incidents, as well as forensics building capacity. All these arrangements contribute to a posture of cyber defence of strength while establishing India as a global leader and partner. Indian engagement in global forums is in alignment with its concern for the evolution of international cyber policy and law. India has been actively engaging in the United Nations Group of Governmental Experts (UN GGE) and Open-Ended Working Group (OEWG) processes, which form the core of the development of norms and rules of responsible behaviour in cyberspace. India has long supported the belief that cyberspace should be regulated by international law in existence today, e.g., the United Nations Charter, and continued to advocate for the creation of a new, comprehensive, and participatory cybercrime convention within the framework of the United Nations. It borrows from India's concern that current treaties such as the Budapest Convention on Cybercrime, to which India is not a signatory, are unbalanced towards developed countries and fail to articulate the fears of the Global South. India's move towards a UN-based treaty for cybercrime is also proof of its bigger diplomatic play in securing equanimity, universality, and respect for local legal orders in international rule-making. Nationally, India has introduced a sequence of policy initiatives complementing its global cyber diplomacy agenda. These include the National Cyber Security Policy (2013), which outlines the vision to secure cyberspace and build national capacity; the Draft National Cyber Security Strategy (2021), which addresses building critical infrastructure, institutional arrangements, and legal frameworks; and the Digital India initiative, which emphasizes safe digital infrastructure and governance. Additionally, proposing the Digital Personal Data Protection Act and trying to modify the Information Technology Act works towards making India's legal system compatible with international practices and protecting personal rights while promoting innovation. These policies work on two fronts: strengthening the national cybersecurity landscape and promoting India as a normative force for responsible digital progress worldwide.<sup>15</sup>

---

14 Government of India, "Digital India: Shaping Global Cyber Norms," (2023), <https://pib.gov.in>.

15 Government of India, "Digital India and Cyber Law Development," (2023), <https://pib.gov.in>.

## Conclusion

The Indian cybercrime law and international cooperation is a complex, multi-dimensional issue reflecting the country's growing digital economy and increasing place in global regulation of cyberspace. India, being among the globe's largest virtual community and a progressively integrated economy, has its own unique challenges policing cybercrime, protecting digital infrastructure, and upholding the safety of its people in the information age. The country's national legal framework, largely established by the Information Technology Act, 2000, and its later amendments, serves as the foundation for controlling cybercrime domestically. Because cybercrime is inherently international, India's ability to effectively combat such crime relies not just on the country's domestic legal and institutional setup but also on the ability to advance international cooperation beyond borders to address such crime. India's reaction to cybercrime legislation is evolving with the ever-changing threats, technological advancements, and growing requirement for international cooperation. India has come a long way in strengthening its jurisprudence, as seen from the expansion of the Information Technology Act and the Digital Personal Data Protection Bill coming into effect. Despite all these advancements, the country still has much to address in enforcement, particularly in rural regions where digital awareness and infrastructure are lacking. Variations between states with regards to technical capabilities, human resources, and effectiveness of law enforcement agencies lead to significant gaps in effectively confronting cybercrime across the country evenly. Moreover, the increasing complexity of cybercrime, such as ransomware attacks, data breaches, and cyber espionage, requires continuous updating of legal provisions, technical tools, and investigation procedures.

International collaboration is crucial in India's fight against cybercrime because cybercriminals typically act internationally, exploiting legal and technological disparities between nations. India's participation in international agreements, such as the efforts of the United Nations to formulate a global instrument on cybercrime, and interaction with regional associations like the Shanghai Cooperation Organisation (SCO) and the ASEAN Regional Forum points towards the nation's inclination to establish international cooperation for enforcement of cyber law. Although India has not ratified the Budapest Convention on Cybercrime, it has been engaged actively in bilateral agreements with other countries for the sharing of threat intelligence, best practices, and coordination of investigations. This shows that India is aware of the role of international cooperation in fighting cybercrime in this highly networked world. India's global contribution to fighting cybercrime through capacity-building initiatives has also expanded. By providing training to law enforcement officers from other developing nations and sharing technological know-how through mechanisms like the Indian Technical and Economic Cooperation (ITEC) program, India is in a strong position to be a regional and international cyber resilience leader. This capacity-building approach not only increases global cooperation but also ensures that nations are in a better position to counter emerging cyber threats. India's role in shaping international cybercrime norms also highlights the need to develop legal frameworks that address the tension between security needs and the protection of individual rights and privacy.

## References

- Bhatia, P. (2019). Cybercrime and its Legal Impact in India. *Law and Society Review*.
- Chakrabarti, S. (2015). *Cyber Crime and the Law in India: Policy, Regulation, and Protection*. LexisNexis India.
- Jain, R. & Sharma, P. (2018). *Cyber Laws in India: An Analysis of Legal Framework*. *International Journal of Law and Legal Jurisprudence Studies*.
- Karnani, A. (2021). *Cybersecurity and the Law: An Indian Perspective*. Sage Publications.
- Goswami, N. (2016). *Cybercrime in India: Laws, Legislation, and Jurisprudence*. *Law Review*.
- Sharma, A. (2020). *Cybercrime Legislation in India and International Cooperation: Challenges and Prospects*. *The Journal of International Law and Policy*.
- Kumar, V. & Singh, S. (2020). *Legal Protection in the Cyber World: A Comprehensive Guide*. Oxford University Press.
- Nadkarni, S. (2017). *Cybercrime and its Regulatory Framework: An International and Indian Context*. *The Indian Journal of Cybersecurity*.
- Bhatia, R. (2016). *The Digital Age and Cybercrime: An Overview of India's Legal Mechanisms*. *Cyber Law Review*.
- Dhillon, G. & Singh, K. (2020). *Global Cybersecurity Cooperation and Indian Policies*. Springer.
- Jain, S. & Rao, R. (2019). *International Cooperation in Cybercrime: The Indian Approach*. *National Cybersecurity Journal*.
- Rao, P. (2021). *The Challenges of Cybercrime Legislation in India and Global Cooperation Efforts*. *Cybercrime Law Quarterly*.
- Saxena, V. (2020). *The Evolution of Cyber Laws in India and Their Global Implications*. *International Journal of Cyber Law*.
- Sharma, P. & Mehra, K. (2017). *Cyber Laws and Regulations: A Global and Indian Perspective*. Cambridge University Press.
- Yadav, N. (2022). *Cybercrime Legislation: A Comparative Study of India and International Norms*. *Legal Insights Journal*.
- Joshi, A. (2018). *Digital Governance and Cybercrime Cooperation: The Case of India*. *The Journal of Global Legal Studies*.
- Hooda, D. (2021). *Cybercrime and Data Protection Laws: India in a Global Context*. *International Cyber Law Review*.
- Batra, S. (2019). *Understanding Cybercrime: The Role of Indian Legislation in Global Cyber Governance*. *World Cyber Law Forum*.
- Sengupta, S. (2020). *Cybercrime in India: Legal Framework and International Challenges*. *Journal of Information Law and Technology*.

- Sharma, D. (2019). Cybercrime Laws in India: Challenges and Global Cooperation. Law and Technology Review.
- Gupta, R. & Kumar, A. (2018). The Cybersecurity Bill in India and Its Global Implications. Legal Research Journal.
- Singh, M. & Rajput, N. (2021). India and International Cybercrime Cooperation: Legal Framework and Implementation. International Cybersecurity Policy Review.
- Patel, V. (2020). Cybercrime, Digital Sovereignty, and India's Position in Global Cooperation. International Journal of Cyber Diplomacy.
- Mehta, R. & Shah, A. (2017). Cybercrime and Data Privacy in India: A Global Legal Perspective. International Cyber Law Journal.
- Bansal, V. & Kapoor, D. (2018). India's Role in Cybercrime Legislation: A Global Perspective. The Journal of International Cyber Law.
- Choudhury, A. (2016). Global Cybersecurity and India's Legal Response: Policy Initiatives and Legal Cooperation. Cyber Law Bulletin.
- Tripathi, R. & Verma, A. (2020). International Cooperation in Cybercrime and India's Legislative Challenges. South Asian Journal of Cyber Law.
- Kumar, S. & Gupta, M. (2019). Cyber Laws and Cybercrime Investigations: A Global Comparison with Indian Legislation. International Cyber Crime Studies.
- Mishra, S. (2020). Legal Approaches to Cybercrime: India's Engagement in Global Cyber Governance. Asian Cybersecurity Review.
- Singh, P. (2018). Cybercrime Law Enforcement in India: Challenges and Global Cooperation. Cybersecurity Law and Policy Journal.