INTERNATIONAL JOURNAL OF PHARMACEUTICAL SCIENCES
[ISSN: 0975-4725; CODEN(USA): IJPS00]
Journal Homepage: https://www.ijpsjournal.com

OPEN ACCESS

**Review Article**

# Transnational Cybercrime: Legal Frameworks, Challenges, And Strategies For Effective Cross-Border Prosecution

**Dr. Dharmendra Kumar***

*Faculty of Law, Shia P G College, Lucknow*

ARTICLE INFO

Published: 4 Sept. 2026
Keywords:
UNCC, Budapest Convention, INTERPOL, IT Act, MLATs, Transnational Cybercrime, Digital Forensics
DOI:
10.5281/zenodo.22305128

## ABSTRACT

The global justice is now being threatened by challenges like transnational cybercrime in the digital era. Criminal activities often cross-national borders, exploiting differences in legal systems, evidentiary standards, and investigative capacities. This makes the identification of criminal acts, as well as cross-border prosecution and judicial cooperation, highly complex and demanding. At the international level, the United Nations Convention against Cybercrime (UNCC, 2024–2025) provides a comprehensive legal framework to harmonize definitions of cybercrime, strengthen investigative collaboration, expedite mutual legal assistance, and facilitate the sharing of digital evidence among states. Partnerships which are operational between INTERPOL and the United Nations Office on Drugs and Crime (UNODC) further support capacity building, intelligence exchange, and coordinated enforcement, forming a multilateral cooperation framework aligned with Mutual Legal Assistance Treaties (MLATs). These arrangements accelerate cross-border investigations and enable more effective international responses to cybercrime. The Budapest Convention on Cybercrime (2001) continues to play a central role in harmonizing substantive and procedural cybercrime laws. It provides standardized offense definitions, facilitates expedited access to evidence, and establishes mechanisms for cross-border cooperation. Nonetheless, challenges persist, including uneven state participation, sovereignty concerns, and variations in data protection and privacy regulations, which limit its overall effectiveness. The legal foundation in India is formed by Information Technology Act, 2000 for addressing cyber offenses and managing digital evidence and recent reforms including the Bhartiya Nyaya Sanhita (BNS) 2023 and the Bharatiya Sakshya Adhiniyam (BSA) 2023, modernize substantive offenses and evidentiary standards. These reforms act towards enhancing the admissibility of electronic and digital forensic evidence and strengthen role of expert testimony in courts, aligning domestic legal procedures with technological realities

***Corresponding Author:** Dr. Dharmendra Kumar
**Address:** *Faculty of Law, Shia P G College, Lucknow*
**Email** ✉: dk535272@gmail.com

**Relevant conflicts of interest/financial disclosures**: The authors declare that the research was conducted in the absence of any commercial or financial relationships that could be construed as a potential conflict of interest.

Despite these frameworks, persistent challenges remain, including jurisdictional differences, technical barriers, resource constraints, and complexities in evidence collection. By harmonizing national and international laws, developing interoperable forensic standards, and strengthening cross-border cooperation, states can implement more effective measures against transnational cybercrime, thereby reinforcing both digital security and the global justice system.

## INTRODUCTION

The internet has become an integral component of almost every aspect of modern life, including education, governance, international relations, communication, and commerce. Cyberspace has provided unprecedented opportunities for individuals and institutions to communicate, collaborate, and exchange resources beyond national boundaries, thereby fostering the growth of skills, knowledge, and innovation on a global scale. However, this rapid digitalization and global interconnectedness have also given rise to several complex challenges, particularly in the legal and regulatory domains.

Among these challenges, cybercrime emerges as one of the most serious and attention-worthy issues, encompassing offences for example, ransomware attacks, phishing, online fraud, breaches of sensitive data, and cyber espionage. Unlike conventional crimes, which are mostly restricted to a specific geographical area or jurisdiction, cybercrimes are inherently borderless in nature. In such cases, the offender, victim, and evidence may simultaneously exist in different countries, making the processes of investigation and prosecution highly complex.

Consequently, the global and decentralized nature of cybercrime not only poses significant obstacles to effective law enforcement but also raises critical concerns regarding jurisdiction, legal coordination, and international cooperation. Therefore, in the digital age, addressing cybercrime necessitates a re-evaluation of traditional legal frameworks and the adoption of a more coordinated global approach.

### Literature Review

The earliest in time international treaty is the *Budapest Convention* directed at harmonizing national cybercrime laws and promoting international cooperation in investigations and prosecutions. The United Nations Guidelines for Combating Cybercrime (2019) set out a framework of voluntary measures designed to combat cybercrime while fostering enhanced international collaboration and coordination among countries.

Kshetri underscores the multifaceted nature of cybercrime in India, noting that the country's cybersecurity environment and its ability to prosecute cyber offenders are influenced by a combination of economic conditions, institutional capacities, and international dynamics. He points to a significant shortfall in tackling cross-border cybercrime and advocates for more nuanced and adaptive policymaking to effectively address these challenges.[1] These studies shed light on the challenges posed by differences in legal system, such as varying definitions of cybercrimes, differences in penalties and sentencing, and variations in the level of enforcement and resources allocated to combating cybercrimes.[2]

[1] Nir Kshetri, Cybercrime and Cybersecurity in India: Causes, Consequences and Implications for Political and Economic Institutions, 66 springer 313, (2016)

[2] Brenner, S. W. (2010). Cybercrime: Criminal Threats from Cyberspace. ABC-CLIO.

Baxi (2020) emphasizes that the transnational nature of cybercrimes, with offenders and victims spread across multiple countries, complicates the determination of jurisdiction and the enforcement of uniform legal standards. Similarly, a study conducted by the National Judicial Academy investigates jurisdictional issues in cybercrime under Bharatiya Nyaya Sanhita, 2023 and also the Information Technology Act, 2000.

**Budapest Convention on Cybercrime**

The Budapest Convention on Cybercrime in 2001 is the initial comprehensive international treaty dealing with cybercrime through a unified legal framework and enhanced cross-border cooperation. It was developed under the auspices of the Council of Europe with the objective of harmonizing national cyber laws, improving investigative techniques, and strengthening international collaboration in combating cyber offences. [3]The Convention recognizes the growing threat posed by cybercrime to the confidentiality, integrity, and accessibility of computer systems, networks, and data, and emphasizes need for a coordinated global response.

A core feature of the Convention is the substantive criminal law framework, which requires member states to criminalize a range of cyber offences. These include unauthorized access to computer systems (hacking)[4], illegal obstruction of non-public transmissions of data[5], data interference like impairing, deleting, or altering computer data, and system interference affecting the functioning of computer systems Additionally, it addresses computer-related offences such as fraud and forgery committed through manipulation of digital data[6], as well as violations of intellectual property rights carried out on a commercial scale using computer systems.[7] The Convention also extends criminal liability to attempts, aiding and abetting, and establishes responsibility for legal persons (corporate liability).[8]

In addition to defining offences, the Convention provides a detailed procedural law framework to facilitate effective investigation and prosecution. It empowers competent authorities to order the expedited preservation of stored computer data, including traffic data, particularly where there is a risk of loss or alteration. It also authorizes search and seizure of computer systems and storage media, and the collection and real-time interception of electronic evidence. These procedural powers are essential for addressing the transnational and volatile nature of digital evidence. However, their application is subject to strict safeguards under domestic law to ensure the protection of fundamental rights, including privacy, due process, and the principle of proportionality.[9]

Another significant pillar of the Convention is its emphasis on international cooperation. Given the borderless nature of cybercrime, the Convention establishes mechanisms for mutual legal assistance, extradition, and the sharing of electronic evidence among states. It encourages the widest possible cooperation in investigations and proceedings related to cyber offences and facilitates timely and efficient exchange of information between national authorities.[10] This cooperative framework is crucial for overcoming

[3] Preamble, Budapest Convention on Cybercrime, 2001.
[4] Article 2, Ibid.
[5] Article 3, Ibid.
[6] Article 8, Ibid.
[7] Article 10, Ibid.
[8] Articles 11–13, Ibid.
[9] Article 15, Ibid.
[10] Chapter III, Ibid.

jurisdictional challenges and ensuring effective enforcement of cyber laws.

Moreover, the Convention integrates human rights considerations into its framework. It mandates that all measures taken under the Convention must come in line with international human rights guidelines, particularly those addressing the protection of privacy and civil liberties.This ensures a balance between effective law enforcement and the safeguarding of individual freedoms.

**Jurisdictional Challenges in Cross-Border Cyber crime**

Cross-border cyber fraud, such as online trading scams, poses unique challenges due to the transnational nature of the internet. Offenders, digital infrastructure, and victims often span multiple countries, complicating the determination of legal jurisdiction.[11] In India, the Information Technology Act, 2000 provides for extraterritorial jurisdiction, but enforcement is hindered by procedural delays, differences in national laws, and technological anonymity such as cryptocurrencies and offshore accounts.[12]

International cooperation through Mutual Legal Assistance Treaties (MLATs), INTERPOL coordination, and emerging multilateral conventions is essential for sharing digital evidence, conducting joint investigations, and extraditing offenders. Harmonized legal standards and robust cross-border mechanisms are therefore critical to ensuring effective enforcement against cybercrime.

**Cross-Border Legal Instruments and Enforcement Strategies in Cybercrime**

The transnational and borderless nature of cybercrime has necessitated the development of comprehensive international legal instruments and coordinated enforcement strategies, as digital offences often span multiple jurisdictions and exploit disparities in national legislation. Historically, the absence of a globally binding cybercrime treaty prompted the United Nations to initiate negotiations for a multilateral convention providing a unified framework for prevention, investigation, prosecution, and international cooperation. In December 2019, a resolution was adopted by the UN General Assembly to negotiate an extensive international treaty dealing with the misuse of information and communications technology (ICT) for criminal motives. These efforts culminated in the United Nations Convention against Cybercrime, officially titled *Strengthening International Cooperation to Combat Crimes Committed by Means of ICT Systems and for the Sharing of Evidence in Electronic Form of Serious Crimes*[13], which was adopted in December 2024 and opened for signature in October 2025 in Hanoi. The convention seeks to harmonize substantive criminal law definitions for cyber offences and establish robust procedural tools and cooperation mechanisms across states. It mandates the criminalization of acts such as unauthorized system access, data interference, online fraud, and the exploitation of children, while promoting the preservation and sharing of electronic evidence, expedited mutual legal assistance, and the

[11] UNODC, *Cybercrime and the Challenges of Transnational Investigations* – global dispersion of offenders, infrastructure, and victims.

[12] INTERPOL, *Cybercrime Operational Handbook 2022* – challenges due to anonymizing technologies, cryptocurrencies, and offshore accounts.

[13] United Nations Convention against Cybercrime, adopted Dec 2024; opened for signature Oct 2025.

extradition of suspects.[14] The treaty also envisages the creation of 24/7 contact points to facilitate rapid cooperation and provides capacity-building support for developing countries to strengthen their legal frameworks and enforcement capabilities.[15] While the convention upholds human rights, critics caution that its broad definitions and procedural powers may pose risks to privacy and civil liberties if not carefully implemented.[16]

Complementing the UN framework, existing mutual legal assistance treaties (MLATs) and bilateral or regional agreements provide cross-border evidence collection, legal cooperation, and extradition in cybercrime matters.[17] These instruments typically require dual criminality, emphasizing the need for harmonized criminal definitions across jurisdictions. Operationally, INTERPOL has a major part in strengthening these legal frameworks by coordinating real-time intelligence sharing, supporting transnational investigations, and enabling joint law enforcement operations.[18] INTERPOL's networks strengthen global responses to common cyber threats, including ransomware, financial cyber fraud, and exploitation crimes, often through organized collaborative operations that dismantle malicious infrastructure and apprehend perpetrators.

Collectively, these treaties, cooperative instruments, and institutional strategies form an evolving international legal architecture for combating cybercrime. They underscore that effective enforcement requires not only harmonized legislation furthermore practical methods for real-time co-operation, evidence sharing, coordinated action among states and law enforcement agencies.

**Indian Legal Framework Against Cybercrime**

India's legal framework for combating cybercrime and financial offences represents a comprehensive integration of specialized legislation, a modernized criminal code, and regulatory oversight, designed to address both traditional and technologically enabled crimes. The Information Technology Act, 2000, as amended in 2008, provides the primary legal foundation for cyber offences, encompassing unauthorized access to computer systems (Section 43), hacking and computer-related fraud (Section 66), identity theft (Section 66C), cheating by personation (Section 66D), violations of privacy (Section 66E), cyber terrorism (Section 66F), and dissemination of obscene material through digital platforms (Sections 67 and 67A). Complementing this, the Bharatiya Nyaya Sanhita (BNS), 2023, which modernizes and consolidates India's criminal law, extends its scope to cyber-enabled offences, covering organized criminal activity (Section 111), terrorism including cyber-terrorist acts (Section 113), and digital fraud through cheating and personation (Sections 318–319), alongside provisions governing forgery, breach of

[14] UN Cybercrime Convention — criminalizes acts such as unauthorized system access, data interference, online fraud, and exploitation of children.

[15] UN Cybercrime Convention, provides 24/7 contact points and capacity-building support for developing countries.

[16] Critiques of the UN Cybercrime Convention — highlight potential risks to privacy and civil liberties due to broad definitions and procedural powers.

[17] Mutual Legal Assistance Treaties (MLATs) and bilateral/regional agreements — enable cross-border evidence collection, legal cooperation, and extradition.

[18] INTERPOL, coordinates international intelligence sharing, supports transnational investigations, and facilitates joint operations against cybercrime.

trust, and economic extortion. In the financial domain, regulatory and statutory measures address money laundering (Sections 3, & 5–8), investor protection, market manipulation, and compliance failures in banking and securities sectors (Sections 11–12) Enforcement and oversight are executed by a combination of cyber and financial authorities, including CERT-In, state cybercrime cells, the 'Securities and Exchange Board of India (SEBI)', the 'Reserve Bank of India (RBI)', and adjudicating officers empowered under the IT Act. Despite this robust framework, challenges remain due to cross-border jurisdictional limitations, rapidly evolving technologies, the rise of cryptocurrency-related frauds, and underreporting of cyber and financial crimes, emphasizing the need for continuous legislative adaptation, enhanced institutional capacity, and public awareness initiatives.

Child protection in the digital context is governed by the Protection of Children from Sexual Offences (POCSO) Act, 2012, which criminalizes sexual exploitation, child pornography, and online grooming of minors, ensuring accountability for offences committed through ICT platforms.[19] Other relevant legislation includes the Negotiable Instruments Act, 1881, which addresses financial frauds involving digital or electronic transactions.[20]

**Significant Judicial Findings and Implications**

**United States v. Albert Gonzalez (2009)**

Albert Gonzalez led a large-scale hacking operation that stole over 170 million credit and debit card numbers from companies like TJX and Heartland Payment Systems between 2005–2007. He used malware and network breaches to obtain the data and sold it on the black market. In 2008, he pled guilty to conspiracy, fraud, identity theft, and computer crimes. In 2009, he was sentenced to 20 years in federal prison and ordered to forfeit millions of dollars, marking one of the most significant cybercrime convictions in U.S. history.

**Sony Pictures Entertainment Hack (2014)**

The hacking community "Guardians of Peace", which is purportedly connected to North Korea, launched a huge cyberattack against Sony Pictures Entertainment in November 2014 as a retribution for the release of a movie The Interview. Tens of terabytes of sensitive material, including executive emails, financial documents, unreleased films, and employee personal information, were stolen and leaked by hackers, who also destroyed certain internal systems. The U.S. government formally attributed the attack to North Korea, and the incident caused financial losses, reputational damage, and operational disruption, while highlighting the urgent need for stronger corporate cybersecurity and raising questions about legal accountability in state-sponsored cyberattacks.

**United States v. Microsoft Corp., 138 S. Ct. 1186 (2018)**

In 2013, the U.S. government served Microsoft with a warrant to access a customer's emails stored on servers in Ireland. Microsoft argued that U.S. law could not compel disclosure of data stored overseas. Lower courts conflicted, but before the Supreme Court could decide, Congress passed the CLOUD Act (2018), clarifying that U.S. providers must comply with warrants for data stored abroad. Consequently, the Supreme Court dismissed the

[19] Sections 11–13 of POCSO Act, 2012 – Sexual offences against children, including online exploitation.

[20] Negotiable Instruments Act, 1881 – offences related to financial frauds involving digital or electronic transactions.

case as moot, vacating lower court rulings. The case highlighted legal challenges of cross-border data access and influenced modern digital privacy and law enforcement practices.

**Carpenter v. United States (2018)**

Supreme Court adjudged that law enforcement agencies should obtain a warrant before gaining access to historical cell phone location data. It acknowledged the need to strike the right balance in this digital age between upholding the rights of individual's privacy and safeguarding the interests of law enforcement.

**Kochi Businessman Loses ₹24.76 Crore in Online Trading Fraud**

A 49-year-old businessman from Kochi lost ₹24.76 crore to a fraudulent online trading platform called Capitalix after being persuaded by scammers, including someone named "Daniel," to transfer money over time with promises of high returns. The scheme ran from March 2023 to August 2025 and was uncovered when he could not withdraw his funds. The Kochi Cyber Police registered an FIR on September 1, 2025, and a Special Investigation Team (SIT) is investigating, including possible links to a Cyprus-based call centre. Several arrests have been made, some funds have been frozen, but as of early 2026, no court judgment or sentencing has been issued, and the case remains under investigation.

**The Development of Digital Forensics Standards**

Digital forensics involves the process of collecting, preserving, and analyzing evidence from digital devices and networks. With the growth of technology and cybercrime, developing standardized digital forensic protocols has become essential. These standards ensure that evidence remains intact, legally admissible, and transparent, while maintaining consistency across investigative agencies. In multi-national frameworks like the Belt and Road Initiative (BRI), they help facilitate secure and lawful data sharing, compliance with data protection regulations, and effective risk management.

Overall, developing digital forensics standards is not just a technical requirement but also a legal, ethical, and strategic necessity, ensuring that digital evidence is reliable, secure, and internationally acceptable.

## CONCLUSION

Transnational cybercrime has emerged as an extremely complex and multi-dimensional challenge in the digital era, as it transcends traditional national boundaries and employs highly advanced technological tools. At the international level, instruments such as the Budapest Convention (2001) and the United Nations Convention against Cybercrime (2024–2025) play a vital part in standardizing definitions of cybercrime, strengthening cross-border cooperation, and facilitating the exchange of digital evidence. Nevertheless, disparities in national legal systems, uneven participation in treaties, jurisdictional conflicts, and concerns regarding privacy and sovereignty continue to pose significant obstacles to effective prevention and prosecution.

In the Indian context, the Information Technology Act, 2000, the Bhartiya Nyaya Sanhita (2023), and the Bharatiya Sakshya Adhiniyam (2023) have strengthened the judicial recognition of cybercrime and digital evidence. Despite this, challenges such as cross-border judicial action, technological complexities, and rapidly evolving cyber threats persist. Judicial rulings, such as United States v. Microsoft Corp. (2018) and

Carpenter v. United States (2018), highlight the critical need to balance digital privacy with law enforcement objectives.

Therefore, addressing transnational cybercrime effectively requires a holistic approach, which includes robust and standardized legal frameworks, interoperable digital forensic standards, institutional capacity building, and multilateral cooperation. Aligning national laws with global standards and strengthening international collaboration will not only enhance cybersecurity in India but also ensure the integrity and effectiveness of the global justice system.

**Suggestions**

1. Establish a coherent and standardized legal framework through the coordination of national cyber laws and international conventions, facilitating smoother and more effective cross-border prosecution processes.

2. Develop interoperable digital forensic standards and protocols to ensure the global admissibility and legal robustness of digital evidence.

3. Formulate clear and technologically informed strategies for prevention, monitoring, and response to emerging technologies, such as cryptocurrencies, AI-based cyberattacks, and ransomware.

4. Enhance the capacity of multilateral cooperation mechanisms like INTERPOL, UNODC, and MLATs to ensure rapid, secure, and coordinated information exchange in cross-border cybercrime investigations.

5. Develop explicit ethical and legal guidelines to safeguard civil privacy, data protection, and human rights within digital investigations and cyber law enforcement.

## REFERENCES


1. Information Technology Act, No. 21 of 2000,
2. Bharatiya Nyaya Sanhita, No. 45 of 2023,
3. Prevention of Money Laundering Act, No. 15 of 2002,
4. Ritu Agarwal, Cross-Border Cybercrime and Jurisdictional Dilemmas in India, 8 Indian J.L. & Tech. 112 (2020).
5. Apar Gupta, The Information Technology Act, 2000: A Legal Review of Cyber Offences in India, 12 Nat'l L. Sch. India Rev. 45 (2021).
6. Ahmed, M. F., & Arifuzzaman, M. (2025). The Future of Cybersecurity and Data Privacy in Bangladesh: Identifying the Legislative Gaps. Asian Journal of Social Sciences and Legal Studies, 347–357.available at: https://doi.org/10.34104/ajssls.025.034700357
7. Ashurov, A. (2024). Jurisdictional Challenges in Cross-Border Cybercrime Investigations. Available at: https://doi.org/10.5281/ZENODO.11234768
8. Siddiqua, Dr. R. (2024). Challenges Faced by Police Officers in Investigating Cyber Crime: An Exploratory Study in Bangladesh. International Journal of Humanities, Social Sciences and Education, 11(7), 150–161. Available at: https://doi.org/10.20431/2349-0381.1107014
9. https://www.interpol.int/en
10. https://legalaffairs.gov.in/mlat
11. https://www.unodc.org


HOW TO CITE: Dr. Dharmendra Kumar, Transnational Cybercrime: Legal Frameworks, Challenges, And Strategies For Effective Cross-Border Prosecution, Int. J. of Pharm. Sci., 2026, Vol 4, Issue 9, 502-509. https://doi.org/10.5281/zenodo.22305128