ADJUDICATING AND INVESTIGATING CROSS-BORDER CYBERCRIMES: A STUDY OF INDIA'S JURISDICTIONAL FRAMEWORK

Priyanandhine Bhaskaran, B.B.A. LL.B., Indian Institute of Management Rohtak

Yashaswi Gole, B.B.A. LL.B., Indian Institute of Management Rohtak

ABSTRACT

Digitalisation has led to various challenges in relation to cybercrimes. Due to globalisation the cybercrimes have transcended beyond the territorial limits. To mitigate those challenges there is a need to develop a comprehensive framework for adjudication and investigation of cybercrime across boundaries. Information Technology Act, 2000, Bharatiya Nyaya Sanhita, 2023 and Bharatiya Nagarik Suraksha Sanhita, 2023 provides for extraterritorial application and power of courts to try offences committed outside India. However, there is still a huge gap in investigation mechanism. Due to heavy reliance on bilateral treaties the issue of slow processing of request in bureaucratic setup is a major setback. Similarly other challenges like privacy concerns, meeting higher legal standards etc. needs to be addressed to bring Indian Practices on par with international standards.

Keywords: cybercrimes, extraterritorial jurisdiction in cyberlaws, cross-border cybercrime investigation, cyberlaws in India.

1. Introduction

The exponential growth of digital connectivity has ushered in unprecedented cybersecurity and law enforcement challenges, particularly in cross-border cybercrime. This challenge is especially pertinent for India, which has recently published the World Cybercrime Index, which ranks as the tenth most significant source of cybercrime globally.[1] This positioning in the global cybercrime landscape and India's status as home to the world's second-largest internet population presents unique challenges and urgencies in addressing cross-border cyber threats.[2]

The scale and sophistication of cybercrime in India have evolved dramatically over the past decade. Statistical evidence reveals a stark escalation in reported cybercrime cases, from approximately 3,500 in 2012 to 66,000 in 2022.[3] This nearly nineteen-fold increase over a decade reflects the growing sophistication of cyber criminals and highlights the expanding attack surface as India's digital economy continues to grow. The financial implications are equally concerning, with the average cost of a data breach in India between 2023 and 2024 reaching 2.35 million US dollars.[4]

Recent incidents underscore the gravity of cross-border cyber threats facing India. The 2022 power grid attack, allegedly perpetrated by a state-sponsored group from China,[5] and the 2023 APT41 attacks targeting multiple Indian sectors, including telecommunications, manufacturing, and information technology, exemplify the sophisticated nature of contemporary cyber threats.[6] These incidents highlight how cybercrime has evolved beyond individual actors to include state-sponsored groups capable of targeting critical infrastructure and key economic sectors.

---

[1] Miranda Bruce et al., *Mapping the Global Geography of Cybercrime with the World Cybercrime Index*, 19 PLoS ONE (2024).
[2]Tanushree Basuroy, *Internet usage in India*, Statista (Sep.18, 2024) https://www.statista.com/topics/2157/internet-usage-in-india/#topicOverview.
[3]Tanushree Basuroy, *Cybercrime Cases Registered Under IT Act in India from 2012 to 2022*, Statista (Dec.6, 2023) https://www.statista.com/statistics/309435/india-cyber-crime-it-act/.
[4]Ani Petrosyan, *Average Cost of Data Breach by Country or Region*, Statista (Sep.24, 2024) https://www.statista.com/statistics/463714/cost-data-breach-by-country-or-region/.
[5]Binayak Dasgupta, *Chinese hackers targeted 7 Indian power hubs, govt says ops failed*, Hindustan Times (Apr.8, 2022) www.hindustantimes.com/india-news/chinese-hackers-targeted-7-indian-power-hubs-govt-says-ops-failed-101649356540330.html.
[6] Khyati Singh, *Decoding Chinese Hacking Syndicate – APT 41*, Centre for Air Power Studies (Aug.4, 2022) https://capsindia.org/decoding-chinese-hacking-syndicate-apt-41/.

The jurisdictional complexities in investigating and prosecuting cross-border cybercrime present significant challenges for law enforcement agencies and judicial systems. A KPMG study reveals that 40 per cent of end users identify cross-country jurisdictional issues as a significant hindrance in lodging complaints with cyber cells.[7] This data further underscores the urgent need for more effective international cooperation frameworks and streamlined investigative procedures.

International frameworks such as the Budapest Convention on Cybercrime, the European Investigation Order (EIO), and the United States Clarifying Lawful Overseas Use of Data (CLOUD) Act, 2018 offer potential models for addressing these challenges through enhanced international cooperation. However, India's absence from key international treaties, particularly the Budapest Convention, creates significant gaps in its ability to conduct efficient cross-border investigations and collect evidence.

The increasing complexity of cross-border cybercrime poses significant jurisdictional challenges for countries like India. Despite having a legislative framework to address cybercrime, India's laws often fail to clarify how to investigate and prosecute offences involving multiple jurisdictions. Furthermore, India's non-participation in vital international treaties, such as the Budapest Convention on Cybercrime, limits its ability to cooperate efficiently with other countries in handling cybercrimes, particularly regarding data sharing, evidence preservation, and extradition. This project explores the gaps in India's legal framework and proposes improvements to align its approach with international best practices for addressing cross-border cybercrimes.

This paper examines these jurisdictional complexities through a comprehensive two-part analysis. The first half explores the fundamental principles governing criminal jurisdiction in cyberspace, analysing Indian legislation and judicial interpretations in dealing with cybercrime. This section mainly focuses on how traditional concepts of territorial and extraterritorial jurisdiction adapt to the unique challenges posed by digital offences.

The latter half delves into the institutional framework for investigating cross-border cybercrimes, analysing India's challenges in accessing cross-border data and comparing

[7] KPMG, *Cybercrime Survey Report, Insights and Perspectives*, KPMG (Dec.14, 2017) https://kpmg.com/ky/en/home/insights_new/2017/12/cybercrime-cybersecurity-law-enforcement-agencies.html.

alternative international models. Through this analysis, the paper aims to identify gaps in India's approach and propose reforms to enhance its capacity to handle cross-border cybercrime more effectively.

The significance of this research lies in its potential to contribute to developing more effective legal and investigative frameworks for addressing cross-border cybercrime in India. As cyber threats evolve and become more sophisticated, the need for robust, internationally coordinated responses becomes increasingly critical. This study's findings and recommendations will be particularly relevant for policymakers, law enforcement agencies, and legal practitioners working at the intersection of technology and criminal justice.

2. Literature review

The rise in cybercrime has necessitated a thorough exploration of jurisdictional frameworks, particularly in the context of cross-border offences. This review synthesises scholarly contributions to understanding the challenges related to jurisdiction, legal frameworks, and enforcement in addressing cybercrime in India while identifying areas for further research.

Kshetri emphasises the complex nature of cybercrime in India, highlighting how economic, institutional, and international factors shape the country's cybersecurity landscape and the prosecution of cybercriminals. He identifies a critical gap in addressing international cybercrimes and calls for a nuanced approach to policymaking that can effectively manage these dynamics.[8] Similarly, a study conducted by the National Judicial Academy investigates jurisdictional issues in cybercrime under both the Indian Penal Code, 1860 (IPC) and the Information Technology Act, 2000 (IT Act). This research provides insights into how Indian courts can exercise jurisdiction over offences committed across borders, calling for more precise legislative definitions of jurisdictional boundaries.[9]

Cross-border data access, a crucial factor in cybercrime investigations, has been explored by the Carnegie Endowment, highlighting the limitations of India's existing Mutual Legal Assistance Treaties (MLATs). The study suggests reforms that could streamline accessing data from foreign jurisdictions, essential in a rapidly evolving technological environment where

[8] Nir Kshetri, *Cybercrime and Cybersecurity in India: Causes, Consequences and Implications for Political and Economic Institutions*, 66 springer 313, (2016).
[9] National Judicial Academy Bhopal, Jurisdictional Issues in Adjudication of Cybercrimes 4 (2022), https://www.nja.gov.in/Concluded_Programmes/2022-23/P-1346%20Programme%20Report.pdf.

timely law enforcement responses are critical.[10] The United Nations Office on Drugs and Crime (UNODC) also addresses the complexities of jurisdiction in cyberspace, arguing that the internet's borderless nature requires more precise legislative measures to help countries like India assert jurisdiction effectively.[11]

To support these legal challenges, Brenner and Koops offer a theoretical framework on jurisdiction, focusing on principles such as active personality, passive personality, and the protective principle. These principles provide a foundation for understanding how states can claim jurisdiction over cybercrimes that impact their nationals or interests, offering guidance for India's approach to cross-border cybercrime legislation.[12]

However, despite these theoretical foundations, practical challenges remain. Research focusing on India's participation in international treaties reveals a gap between policy frameworks and actual implementation. Bureaucratic hurdles and vague legal provisions often obstruct effective cross-border cybercrime prosecutions.[13] These issues are exacerbated by the lack of empirical studies focusing on how Indian authorities navigate jurisdictional complexities in real-world scenarios, with most research tending to emphasise theoretical frameworks rather than practical enforcement issues. International cooperation is also vital in this context, with scholars emphasising that unified approaches are essential for enforcing laws across borders. Countries like India may struggle to prosecute cybercriminals from other jurisdictions without effective collaboration.[14]

The challenges faced by Indian law enforcement agencies in investigating and prosecuting cybercrimes are significant. Vinay K.'s research identifies obstacles such as insufficient training, jurisdictional hurdles, privacy concerns, and outdated legal frameworks. He proposes solutions that include establishing specialised cybercrime units, cross-border collaboration, and

[10] Smriti Parsheera and Prateek Jha, Cross-Border Data Access for Law Enforcement: What Are India's Strategic Options? (Carneige India, 2020), https://carnegie-production-assets.s3.amazonaws.com/static/files/ParsheeraJha_DataAccess.pdf? [hereinafter Cross Border Data Access for Law Enforcement, India].
[11] Karnika Seth, *Evolving Strategies for the Enforcement of Cyberlaws*, KarnikaSeth.com (Jan.31,2010) https://www.unodc.org/e4j/en/cybercrime/module-7/key-issues/sovereignty-and-jurisdiction.html.
[12] Susan W. Brenner and Bert-Jaap Koops, *Approaches to Cybercrime Jurisdiction*, 4 High Tech. L.J., (2005) https://www.researchgate.net/publication/228198888_Approaches_to_Cybercrime_Jurisdiction.
[13] Aseen Chandra Paliwal and Afkar Ahmad, *Emerging Technologies and Future Challenges in Indian Cyber Law*, in *Proceedings of Cybercrime regulations and security- contemporary issues and challenges* (2024).
[14] Mallavarapu Srinija and Samaira Singh, *International Cooperation in Cybercrime Investigation; Analyse the Role of International Collaboration and Treaties in Tackling Cross Border Cybercrimes Involving India*, 9 International Journal for Novel Research and Development a270, (2024).

updates to legislation, all of which could strengthen India's cybercrime enforcement capabilities.[15] Dr. Abhijeet Deb also examines these challenges, focusing on how Indian courts have handled cases involving hacking, cyber terrorism, and data manipulation under the IT Act 2000. His analysis of landmark cases reveals the difficulties involved in cross-border prosecutions, particularly in establishing clear jurisdiction.[16]

Similarly, Ishan Atrey's work delves into the legal implications of digital evidence and privacy concerns in cybercrime cases. He argues that evolving technologies such as cloud computing and cryptocurrencies require reevaluating traditional jurisdictional concepts, emphasising that legal reforms are needed to address these challenges.[17] This perspective aligns with broader calls for integrating domestic legislation with international agreements to create a comprehensive strategy for combating cross-border cyber offences. Therefore, public policy responses to cybercrime must involve both domestic and international approaches to ensure adequate protection for victims and accountability for perpetrators.[18]

In conclusion, while significant strides have been made in understanding the jurisdictional frameworks surrounding cross-border cybercrime in India, there remains a critical gap in empirical research focused on real-world enforcement challenges. Future studies should explore specific case studies and evaluate the effectiveness of existing legal instruments in facilitating cross-border cooperation while also considering the role of emerging technologies in complicating traditional jurisdictional boundaries.

3. Determining Adjudicatory Jurisdiction in Cross Border Cybercrimes

The emergence of cyberspace as a borderless domain has presented unprecedented challenges to traditional legal frameworks, particularly in establishing jurisdiction over cybercrimes that transcend national boundaries. The inherent nature of cybercrimes, which often involve multiple jurisdictions and complex chains of causation, necessitates a comprehensive understanding of theoretical foundations and practical legal mechanisms. This section

[15] Vinay K., *Challenges Faced by Law Enforcement Agencies in Investigating and Prosecuting Cybercrimes in India*, International Journal of Legal Research and Analysis, (2024).
[16] Abhijeet Deb, *Cybercrime and Judicial Response in India*, 3 Indian Journal of Law and Justice 106, (2012).
[17] Ishan Atrey, *Cybercrime and its Legal Implications: Analysing Jurisdiction, Privacy, and Digital Evidence*, 10 International Journal of Research and Analytical Reviews 183, (2023).
[18] Soumyo D. Moitra, *Developing Policies for Cybercrime Some Empirical Issues*, 13 European Journal of Crime, Criminal Law and Criminal Justice 435, (2005).

examines the theoretical foundations, legislative provisions, and judicial interpretations governing jurisdictional aspects of cross-border cybercrimes in India.

3.1 Foundational Principles of Criminal Jurisdiction

To comprehend the complexities of cybercrime jurisdiction in India, it is essential to first delve into the underlying principles that govern criminal jurisdiction in the country. These principles, deeply rooted in legal tradition and international norms, form the foundation upon which the legal framework for addressing cybercrimes has been built.

The primary principle governing criminal jurisdiction in India is the territorial principle, which asserts that a state can prosecute crimes within its territorial boundaries.[19] This principle is a fundamental aspect of national sovereignty. It has been a cornerstone of criminal jurisdiction for centuries, although this application is viewed to be restricting the state's ability to take cognisance of multijurisdictional matters.[20] In the context of traditional crimes, applying the territorial principle is relatively straightforward. However, the borderless nature of cybercrimes presents significant challenges to its application, necessitating a more nuanced approach when dealing with digital offences.

The territorial principle is complemented by the nationality principle, also known as the active personality principle. This principle extends a state's jurisdiction to its citizens, regardless of where they commit offences.[21] This principle is based on the notion that individuals owe allegiance to their home state and should be accountable to its laws even when abroad.[22] In the context of cybercrimes, the nationality principle becomes particularly relevant, allowing India to prosecute its nationals for digital offences committed outside its territorial boundaries. This principle can be instrumental when extradition is difficult or impossible, ensuring that Indian citizens cannot evade justice simply by operating from foreign jurisdictions.

Another crucial principle in the realm of cybercrime jurisdiction is the effects doctrine, also known as the objective territorial principle. This doctrine allows a state to claim jurisdiction

[19] Rollin M. Perkins, *The Territorial Principle in Criminal Law*, 22 Hastings L. J. 1155, (1971).
[20] Wendell Berge, *Criminal Jurisdiction and The Territorial Principle*, 30 Mich. L. Rev. 238, (1931).
[21] Rome Statute of the International Criminal Court, July 17, 1998, 2187 U.N.T.S. 90; Deen-Racsmány, Zsuzsanna, *The Nationality of the Offender and the Jurisdiction of the International Criminal Court*, 95 The Am. J. Int'l L. 606, (2001).
[22] Deen-Racsmány, Zsuzsanna, *The Nationality of the Offender and the Jurisdiction of the International Criminal Court*, 95 The Am. J. Int'l L. 606, (2001).

over an offence if its effects are felt within its territory, even if the act itself was committed elsewhere.[23] The effects doctrine is particularly significant in cybercrimes, where the perpetrator and the victim may be located in different jurisdictions. For instance, if a hacker located outside India launches an attack that impacts computer systems within India, the effects doctrine would allow Indian courts to claim jurisdiction over the case. This principle recognises that in an interconnected digital world, the impact of a crime can be felt far from its point of origin.

The protective principle is yet another concept that comes into play when dealing with cybercrimes. This principle allows a state to claim jurisdiction over offences committed outside its territory if they threaten the state's security or other vital interests.[24] In the context of cybercrimes, this could potentially apply to attacks on critical infrastructure, government systems, or other assets deemed crucial to national security. The protective principle acknowledges that certain offences, even when committed abroad, can significantly impact a state's interests that warrant extraterritorial jurisdiction.[25]

Lastly, the passive personality principle, though not widely recognised in international law, asserts that a state may claim jurisdiction over offences committed against its nationals, regardless of where the offence occurred.[26] While this principle is not explicitly incorporated into India's cybercrime laws, it could potentially be relevant in cases involving Indian citizens victimised in digital spaces. The passive personality principle emphasises the state's responsibility to protect its citizens, even when subject to crimes beyond its territorial boundaries.[27]

These principles of jurisdiction, while distinct, often overlap and interact in complex ways when applied to cybercrimes. The territorial principle may be invoked when any part of a cybercrime occurs within India's borders, even if the perpetrator is located elsewhere. The nationality principle could come into play if an Indian citizen commits a cybercrime abroad.

---

[23] Darrel C. Menthe, *Jurisdiction in Cyberspace: A Theory of International Spaces*, 4 Mich. Telecomm. & Tech. L. Rev. 69, (1998).
[24] *Id* at 7.
[25] Robert Staal, *International Conflict of Laws: The Protective Principle in Extraterritorial Criminal Jurisdiction*, 15 U. Miami L. Rev. 428, (1961).
[26] John G. McCarthy and Darrel C. Menthe, *The Passive Personality Principle and ITS Use in Combating International Terrorism*, 13 Fordham Int'l L. J. 298 (1989); Geoffrey R. Watson, *The Passive Personality Principle*, 28 Texas, (1993); Darrel C. Menthe, *Jurisdiction in Cyberspace: A Theory of International Spaces*, 4 Mich. Telecomm. & Tech. L. Rev. 69, (1998).
[27] Geoffrey R. Watson, *The Passive Personality Principle*, 28 Texas, (1993).

The effects doctrine might be applied if a cybercrime committed outside India has significant impacts within the country. The protective principle could be relevant in cyberattacks targeting critical national infrastructure, while the passive personality principle might be considered in cases where Indian citizens are victimised in virtual spaces.

3.2 Indian Legal Framework Governing Cybercrime Jurisdiction

The legal framework for cybercrime jurisdiction in India is primarily derived from three critical pieces of legislation: IT Act, the Bharatiya Nyaya Sanhita, 2023 (BNS) and the Bharatiya Nagarik Suraksha Sanhita, 2023 (BNSS). These laws and judicial interpretations through landmark cases form the backbone of India's approach to cybercrime jurisdiction.

i. IT Act: Key Jurisdictional Provisions:

The IT Act, enacted in 2000 and amended in 2008, is India's primary legislation dealing with cybercrimes. The Act's jurisdictional provisions demonstrate a conscious effort to address the cross-border nature of cybercrimes. Section 1(2) of the IT Act establishes the concept of extraterritorial application, extending its reach to offences or contraventions committed outside India by any person. Significantly, the nationality of the offender is not a limiting factor in the application of the Act.

Section 75 of the IT Act further clarifies the jurisdictional scope, extending to any offence or contravention committed outside India by any person, irrespective of nationality, provided the act or conduct involves a computer, computer system, or computer network located in India. This section effectively adopts the effects doctrine, focusing on the crime's impact rather than the perpetrator's location. It provides a broad basis for Indian courts to claim jurisdiction over cybercrimes that affect Indian computer resources, regardless of where the perpetrator is located.

ii. BNSS: Implications for Cybercrime Jurisdiction

Chapter XIV of the BNSS deals with the jurisdiction of criminal Courts in India for inquiries and trials, establishing several fundamental principles that become particularly relevant in the context of cybercrimes. Although these provisions were initially drafted with traditional crimes in mind, they have also been interpreted and applied to cybercrimes.

Section 197 establishes the fundamental principle that every offence should be inquired into and tried by a Court within its jurisdiction.[28] This basic rule is supplemented by various provisions addressing more complex scenarios. Section 198 extends jurisdiction to cases where the place of occurrence is uncertain or where the offence is continuing in nature.[29] In such cases, courts having jurisdiction over each area shall be competent to try the offence. This provision is particularly relevant to cybercrimes, which often span multiple jurisdictions.

Section 199 of the BNSS is especially significant in the context of cybercrimes as it embodies the effects doctrine.[30] It provides that when an offence's consequences form part of the offence itself, courts having jurisdiction over the area where such consequences ensue shall have jurisdiction to try the offence. The Supreme Court, in State of Madhya Pradesh v Suresh Kaushal (2001),[31] interpreted this section to mean that both the Court where the act was done and the Court where the consequence ensued have jurisdiction. This interpretation is particularly relevant to cybercrimes, where the act (e.g., launching a cyberattack) and its consequences (e.g., data breach or system damage) often occur in different locations.

The Sanhita demonstrates particular foresight in Section 202, explicitly addressing offences committed through electronic communications, allowing jurisdiction where messages are either sent or received.[32] This provision has become increasingly relevant in the digital age, providing a basis for establishing jurisdiction in cases involving electronic communications, recognising that both the origin and destination of electronic communications can be relevant in determining jurisdiction.

Sections 204[33] and 208[34] of the BNSS address special circumstances, with Section 204 providing for the place of trial of offences triable together and Section 208 establishing procedures for offences committed outside India. The latter provision requires prior sanction from the Central Government, though as clarified in Thota Venkateswarlu v. State of AP (2008),[35] such sanction is not required at the cognisance stage.

[28] Bharatiya Nagarik Suraksha Sanhita 2023, No. 46 of 2023, § 197 (Ind.).
[29] Bharatiya Nagarik Suraksha Sanhita 2023, No. 46 of 2023, § 198 (Ind.).
[30] Bharatiya Nagarik Suraksha Sanhita 2023, No. 46 of 2023, § 199 (Ind.).
[31] State of Madhya Pradesh v. Suresh Kaushal, 2001 (2) ALD (CRI) 330 (Ind.).
[32] Bharatiya Nagarik Suraksha Sanhita 2023, No. 46 of 2023, § 202 (Ind.).
[33] Bharatiya Nagarik Suraksha Sanhita 2023, No. 46 of 2023, § 204 (Ind.).
[34] Bharatiya Nagarik Suraksha Sanhita 2023, No. 46 of 2023, § 208 (Ind.).
[35] Thota Venkateswarlu v. State of A.P. TR. PRINCL., AIR 2011 SUPREME COURT 2900 (Ind.).

iii. BNS: Applicability to Cybercrime Jurisdiction

The BNS extends jurisdiction through Section 1(5), which provides three specific circumstances where offences committed outside India may be tried under Indian law.[36] Of particular relevance to cybercrimes is Section 1(5)(c), which extends jurisdiction to offences committed outside India targeting computer resources within India: *"The provisions of this Sanhita shall also apply to any offence committed by….any person in any place without and beyond India committing offence targeting a computer resource located in India".*[37]

3.3 Judicial Precedents Interpreting Cybercrime Jurisdiction in India

Indian courts have developed a sophisticated approach to jurisdictional issues in cybercrime cases through various landmark decisions. In Vishnu Dutt Sharma and Ors. v. State (1994), the Supreme Court established that the presence of some aspects of an offence within India is sufficient to establish jurisdiction, even if other elements occur abroad.[38] The Court observed that:

"(6) I have been taken through the complaint as also the statement of the complainant. Looking at the allegations contained therein it cannot be said that no offence is made out, nor it can be said that the offence was committed only outside India. Therefore, I am of the considered view that the proceedings cannot be thrown out on the basis of Section 188 CrPC."

This principle was further elaborated by Lee Kun Hee and Ors. v. State of UP and Ors. (2012), where the Court affirmed jurisdiction over offences partially committed in India.[39] This decision is particularly relevant to cybercrimes, often involving actions and consequences spanning multiple jurisdictions. It reinforces the idea that even the partial commission of an offence within India is sufficient to establish jurisdiction.

The case of Mobarak Ali Ahmed v. State of Bombay (1957) provides essential guidance on the application of Section 179 of the Code of Criminal Procedure, 1973 (CrPC) in cases involving remote communications.[40] The Supreme Court held that representations made through letters,

[36] Bharatiya Nyaya Sanhita 2023, No. 45 of 2023, § 1(5) (Ind.).
[37] Bharatiya Nyaya Sanhita 2023, No. 45 of 2023, § 1(5)(c) (Ind.).
[38] Vishnu Dutt Sharma v. State, 1994 SCC OnLine Del 406 (Ind.).
[39] Lee Kun Hee v. State of U.P., AIR 2012 SCW 1316 (Ind.).
[40] Mobarak Ali Ahmed v. State of Bombay, AIR 1957 SC 857 (Ind.).

telegrams, and telephone calls from abroad to victims in India constituted offences triable in India. This principle has direct application to cybercrimes involving similar remote communications.

The question of which Court within India has jurisdiction in cases of cross-border cybercrimes was addressed in Om Hemrajani v. State of UP and Ors (2005).[41] The Supreme Court held that for offences committed abroad (but triable in India), the complainant or victim may approach any court convenient to them in India. This decision aims to facilitate more accessible access to justice for victims of cybercrimes, recognising the potential hardships that could arise if victims were required to approach courts in specific jurisdictions.

In cases where multiple offences are committed across different jurisdictions, the Delhi High Court in Lalitha Lakshmanan v. Central Bureau of Investigation (2017)[42] observed that when offences are allegedly committed by an Indian citizen both within the country and outside, courts where the offence was committed in India and where the accused is found upon being brought to India would have territorial jurisdiction. This decision provides guidance on handling complex cases involving multiple offenses across different jurisdictions, a scenario uncommon in cybercrime cases.

3.4 International Framework and Cooperation: The Budapest Convention on Cybercrime

The most significant international treaty dealing with cybercrimes is the Budapest Convention on Cybercrime, also known as the Budapest Convention. Adopted by the Council of Europe in 2001, it is the first binding multilateral treaty to address internet and computer crime by harmonising national laws, improving investigative techniques, and increasing cooperation among nations.[43] Twenty-two years later, the most relevant international agreement on cybercrime and electronic evidence remains. The Budapest Convention is a criminal justice treaty that provides states with (i) the criminalisation of a list of attacks against and by employing computers[44] and (ii) procedural law tools to make the investigation of cybercrime and the securing of electronic evidence concerning any crime more effective and subject to the

[41] Om Hemrajani v. State of U.P., AIR 2005 SC 392 (Ind.).
[42] Lalitha Lakshmanan v. Central Bureau of Investigation, (2017) 236 DLT 588 (Del. HC).
[43] Convention on Cybercrime, Nov. 23, 2001, Council of Europe, ETS No. 185.
[44] Convention on Cybercrime art. 2-13, Nov. 23, 2001, Council of Europe, ETS No. 185.

rule of law safeguards;[45] and (iii) international police and judicial cooperation on cybercrime and e-evidence.[46] The Council of Europe's Chart of signatures and ratifications of the Convention on Cybercrime (ETS No. 185) shows that on 27 January 2023, the total number of ratifications/accessions was 68, of which India is not a part.[47] While India is not a signatory to the Budapest Convention, the principles embodied in this treaty have influenced India's approach to cybercrime legislation and international cooperation.

The Convention addresses jurisdiction issues in Article 22, which requires member nations to establish jurisdiction over offences committed in their territory, on ships flying their flag, on aircraft registered under their laws, or by their nationals.[48] The Convention also promotes the principle of *aut dedere aut judicare* (meaning to either extradite or prosecute), encouraging countries to assert jurisdiction over offences committed by their nationals even when the offence is committed abroad.

This means that member nations benefiting from such a jurisdictional structure can be confident that no cybercrime can go unpunished due to territorial or other jurisdictional limits. The member states enjoy the power to enforce the law for crimes committed within their territory, by their citizens, or concerning their ships and planes. It also lessens the chances of cybercriminals having "safe havens" as they cannot run away to countries that do not have the offence. In addition, promoting uniform legal standards among the member countries facilitates easier collaboration in the fight against cybercrime and evidence collection between the countries in prosecuting such crimes.

However, India is not a signatory to the Budapest Convention, which implies that India is missing out on these advantages by refusing to join. Devoid of the Convention's provisions dealing with extraterritoriality, India has to face difficulties in dealing with crimes committed by Indians in a foreign country, especially when such crime involves several jurisdictions. In the case of India, the lack of the *aut dedere aut* judicare principle implies that there is no way of forcing another state to deport a wanted criminal and help in giving out justice, hence increasing the duration of such cases. Given that there is no institutional framework under the

[45] Convention on Cybercrime art. 14-21, Nov. 23, 2001, Council of Europe, ETS No. 185.
[46] Convention on Cybercrime art. 23-35, Nov. 23, 2001, Council of Europe, ETS No. 185.
[47] Council of Eur., Chart of Signatures and Ratifications of Treaty 185: Convention on Cybercrime (Jan. 27, 2023) (available at https://www.coe.int/en/web/conventions/full-list?module=signatures-by-treaty&treatynum=185).
[48] Convention on Cybercrime art. 22, Nov. 23, 2001, Council of Europe, ETS No. 185.

Convention, speeding up communication between domestic legal actors is impossible, as they have to rely on international treaties that are usually bilateral and, therefore, take longer to negotiate. India's position outside the Convention hampers its capacity to prosecute and investigate effective cross-border cybercrimes and participate in international cybercrime collaboration.

4. Framework for Cross-Border Cybercrime Investigations

4.1 Current Legal and Institutional Mechanism for Cybercrime Investigation in India

India has established a comprehensive framework to address the growing challenges of cybercrime, particularly those with cross-border implications.[49] The Indian Cybercrime Coordination Centre (I4C), established by the Ministry of Home Affairs (MHA) in New Delhi on 5 October 2018, serves as the cornerstone of this framework, aiming at providing a coordinated ecosystem for law enforcement agencies (LEAs) to combat cybercrimes effectively.[50] This initiative is complemented by the National Cybercrime Reporting Portal, which facilitates easy reporting of cybercrime incidents by the public. The portal's design ensures that reported incidents are automatically routed to the relevant State or Union Territory law enforcement agencies, streamlining the response process.

The effectiveness of these mechanisms is evident in the substantial number of cybercrime incidents reported. Between 1 January 2020 and 7 December 2022, over 16 lakh (1.6 million) cybercrime incidents were reported, resulting in more than 32,000 First Information Reports (FIRs) being registered.[51] This data underscores India's cybercrime challenge and the critical importance of robust reporting and response mechanisms.

The government has issued the National Information Security Policy and Guidelines (NISPG) 2019 to enhance cybersecurity and prevent information security breaches. This policy framework has been disseminated to Central Ministries, State Governments, and Union

[49] Ministry of Home Affairs, Gov't of India, Lok Sabha Unstarred Question No. 1044 (Dec. 13, 2022), (available at: https://www.mha.gov.in/MHA1/Par2017/pdfs/par2022-pdfs/LS-13122022/1044.pdf).
[50] Ministry of Home Affairs, Details about Indian Cybercrime Coordination Centre (I4C) Scheme (2022), https://www.mha.gov.in/en/division_of_mha/cyber-and-information-security-cis-division/Details-about-Indian-Cybercrime-Coordination-Centre-I4C-Scheme.
[51] Ministry of Home Affairs, Cybercrimes and Frauds (2022), https://pib.gov.in/PressReleseDetailm.aspx?PRID=1883066&reg=3&lang=1

Territories, with directives to implement measures for strengthening information security controls and preventing breaches in Information and Communication Technology (ICT) infrastructure.[52]

4.2 Cross-Border Data Access and Mutual Legal Assistance

The transnational nature of cybercrimes presents unique challenges in investigation and prosecution, particularly concerning data access across jurisdictions. A complex interplay of local laws in both the requesting and requested countries governs this aspect of cybercrime investigation. Often, these laws impose stringent limitations on foreign entities' access to personal data, including government agencies, creating significant hurdles for cross-border investigations.

India relies heavily on bilateral treaties known as MLATs to navigate these legal complexities. The MLAT is a treaty-based mechanism that facilitates international cooperation in preventing, suppressing, investigating, and prosecuting crimes by seeking foreign law enforcement assistance in support of ongoing criminal investigations or proceedings.[53] As of 2019, India had entered into MLATs with 42 countries, significantly enhancing its capacity to address cross-border cybercrimes. Expanding this network of treaties reflects India's proactive approach to international cooperation in combating cybercrime.[54]

The scope of assistance provided through MLATs is comprehensive, encompassing:[55]

a. Identification and location of persons and objects.

b. Evidence collection and statement procurement.

c. Facilitation of witness appearances.

[52] Ministry of Home Affairs, Gov't of India, National Information Security Policy and Guidelines, Version 5 (Oct. 9, 2014), (available at: https://barnala.punjabpolice.gov.in/wp-content/uploads/2022/03/06-National-Information-Security-Policy-and-Guidelines-v5.0.pdf).
[53] T. Markus Funk, Mutual Legal Assistance Treaties and Letters Rogatory: Obtaining Evidence and Assistance from Foreign Jurisdictions (Fed. Jud. Ctr., 2d ed. 2024), available at https://ssrn.com/abstract=4623886
[54] Ministry of Home Affairs, Gov't of India, Comprehensive Guidelines for Investigation Abroad and Issue of Letters Rogatory (LRs)/Mutual Legal Assistance (MLA) Request and Service of Summons/Notices/Judicial Documents in Respect of Criminal Matters, F. No. 25016/52/2019-LC (Dec. 4, 2019) (available at https://www.mha.gov.in/sites/default/files/2022-08/ISII_ComprehensiveGuidelines16032020.pdf).
[55] *Id.*

d. Service of judicial documents.

e. Execution of searches and seizures.

f. Provision of information, documents, and evidentiary items.

g. Measures for identifying, locating, and freezing proceeds of crime.

h. Restitution of embezzled public funds.

i. Property delivery and exhibit lending.

j. Protection and preservation of computer data.

This wide-ranging scope demonstrates the potential of MLATs in addressing various aspects of cybercrime investigations. However, the effectiveness of these treaties in practice often depends on the efficiency of the requesting and requested countries' bureaucratic processes and the alignment of their legal systems and priorities.

India is also a signatory to the following international conventions that include provisions for mutual legal assistance as of 2019:[56]

(i) United Nations Convention Against Transnational Organised Crime (2000)

(ii) United Nations Convention Against Corruption (2003)

(iii) United Nations Convention Against Illicit Traffic in Narcotic Drugs and Psychotropic Substance (1988)

(iv) Hague Convention

(v) South Asian Association for Regional Cooperation (SAARC) Convention

(vi) Commonwealth Scheme (Harare Scheme)

[56] *Id* at 15.

4.3 Data Preservation and Investigative Challenges

A critical aspect of cybercrime investigation is preserving digital evidence, which is often volatile and easily alterable. Recognising this challenge, India participates in the G8 24/7 Network for data preservation. The G8 24/7 Network is a system of points of contact established by the G8 countries, a group of 80 countries, to facilitate urgent international cooperation in investigations involving electronic evidence related to high-tech crimes.[57] This network operates 24 hours a day, seven days a week, allowing law enforcement agencies to seek assistance from their foreign counterparts quickly. This network is a crucial channel for expediting data preservation requests, allowing law enforcement agencies to secure potential evidence before it is lost or altered.

The primary purpose of the G8 24/7 Network is to preserve electronic data for subsequent transfer through mutual legal assistance channels. It aims to address the challenges posed by high-tech crimes, which require rapid action from investigators to secure evidence and locate suspects. By providing a structured mechanism for communication, the network enhances traditional methods of cooperation, enabling law enforcement officials to request immediate assistance from foreign jurisdictions, often involving Internet Service Providers (ISPs) to freeze relevant data swiftly.[58] Participants in this Network have pledged to do their utmost to ensure that ISPs freeze relevant information quickly and to provide requested data as efficiently as possible. However, the ability to fulfil these requests may be influenced by each Participant's legal frameworks, technical capabilities, or available resources. The process is also governed by MLATs or Letters of Request, which outline the formal procedures for exchanging evidence between countries.

In India, the Central Bureau of Investigation (CBI) acts as the contact point for this network.[59] The process typically involves an initial 90-day preservation period, during which investigating agencies must initiate formal requests for obtaining the preserved data. This timeframe underscores the time-sensitive nature of cybercrime investigations and the need for swift

[57] G8, 24/7 Network of Contact Points Protocol Statement (available at https://www.combattingcybercrime.org/files/virtual-library/international-cooperation/the-g8-24-7-network-of-contact-points-%28protocol-statement%29.pdf).
[58] Cross Border Data Access for Law Enforcement, India, *supra* note 10 at 4.
[59] Ministry of Home Affairs, Guidelines on Mutual Legal Assistance in Criminal Matters (2022) https://pib.gov.in/PressReleseDetailm.aspx?PRID=1883066&lang=1&reg=3.

international cooperation.

The legal standards for obtaining different types of data vary, reflecting the balance between investigative needs and privacy concerns:[60]

(i) Subscriber Information: This requires establishing the relevance of the evidence to the criminal investigation. It is the lowest legal standard, reflecting primary subscriber data's relatively low privacy implications.

(ii) Transactional Information: Obtaining this data necessitates providing specific facts detailing the relevance and materiality of the records to the investigation. This higher standard acknowledges the more sensitive nature of transactional data, which can reveal patterns of behaviour and associations.

(iii) Content Data: This often requires meeting the highest legal standards, including probable cause and verifying the facts supporting the request. The stringent requirements for content data reflect its susceptible nature and the significant privacy implications of accessing such information.

4.4 Evaluating the Strengths and Gaps in India's Cybercrime Framework

While India's framework for addressing cross-border cybercrimes is comprehensive, its effectiveness is hampered by several challenges. The sheer volume of cybercrime incidents reported through the National Cybercrime Reporting Portal which was over 16 lakh (1.6 million) between 1 January 2020 and 7 December 2022 underscores the magnitude of this challenge.[61] However, the discrepancy between reported incidents and registered First Information Reports (FIRs) (only 32,000 in the same period) raises questions about the system's capacity to process and investigate all reported cases effectively.[62]

Despite an increase in cases and chargesheets filed, rising from 5,180 cases in 2017 to over

[60] *Id.*
[61] Ministry of Home Affairs, Cybercrimes and Frauds (2022), https://pib.gov.in/PressReleseDetailm.aspx?PRID=1883066&reg=3&lang=1.
[62] *Id.*

18,000 in 2021, the number of convictions has not improved significantly.[63] 2017 there were only 152 convictions, which increased slightly to over 490 in 2018. However, the numbers fluctuated in subsequent years, with 360 convictions in 2019 and approximately 1,109 in 2020. By 2021, the situation worsened again, with only 490 convictions recorded. Acquittals have also been notable, with figures ranging from 447 to 627 each year, while the others remain on trial or, in many cases, not even brought for trial for want of evidence.

One of the primary challenges lies in the jurisdictional complexities inherent in cross-border cybercrimes. The borderless nature of cyberspace often conflicts with the territorial jurisdiction of law enforcement agencies, leading to delays and jurisdictional disputes. This mismatch is particularly pronounced in cases where the perpetrator, the victim, and the digital infrastructure used in the crime are located in different countries.

The reliance on MLATs, while necessary for international cooperation, presents its own challenges. The MLAT process is often time-consuming, with average response times ranging from 6 to 24 months. This delay can be particularly problematic in cybercrime investigations, where digital evidence is often time-sensitive. Moreover, the effectiveness of MLATs is limited by varying legal standards and definitions of cybercrimes across different jurisdictions. For instance, what constitutes a cybercrime in one jurisdiction may not be considered illegal in another. This lack of harmonisation in cybercrime laws across nations can create safe havens for cybercriminals and impede effective prosecution.

While theoretically robust, the framework for data preservation and access faces practical implementation challenges. The process of obtaining data through MLATs after its preservation is often hindered by bureaucratic processes and conflicting data protection laws in different jurisdictions. Indian law enforcement agencies frequently encounter situations where preserved data becomes inaccessible due to conflicts with foreign data protection regulations or the expiration of preservation orders before the completion of MLAT processes.[64]

[63] Anupriya Chatterjee, *Why are Cybercrime Convictions Low in India? Weak forensics, Dark Net & Cross-border Attacks,* ThePrint (Dec. 21, 2011) https://theprint.in/tech/why-are-cybercrime-convictions-low-in-india-weak-forensics-dark-net-cross-border-attacks/1273191/.
[64] Amber Sinha et al., *Cross Border Data-Sharing and India A Study in Processes, Content and Capacity* The Centre for Internet and Society (Sept. 27, 2018) https://cis-india.org/internet-governance/files/mlat-report.

Another significant challenge is the shortage of specialised cybercrime units and skilled personnel within law enforcement agencies. While efforts have been made to enhance technical capabilities, there remains a significant gap in the specialised skills required for effective cybercrime investigations, particularly in complex, cross-border cases.[65]

The rapid pace of technological advancement further compounds these challenges, with existing legal and procedural frameworks often struggling to keep pace with emerging technologies and new forms of cybercrime. This creates a situation where law enforcement agencies are constantly playing catch-up, trying to adapt their investigative techniques and legal tools to address novel cyber threats.

4.5 Global Benchmarks: Comparative Approaches to Cybercrime Investigations

Compared to international best practices, India's framework for addressing cross-border cybercrimes reveals several areas for potential improvement. For instance, the European Union's (EU) approach offers a more streamlined mechanism for cross-border investigations. The EIO allows for direct cooperation between judicial authorities of EU member states, significantly reducing the time required to obtain evidence across borders.[66] On the other hand, India heavily relies on separate agreements with each country.

The Budapest Convention on Cybercrime provides another comprehensive framework for international cooperation. This Convention includes provisions for expedited preservation of stored computer data,[67] expedited preservation and partial disclosure of traffic data,[68] real-time collection of traffic data,[69] and establishment of a 24/7 network of contact points for international cooperation.[70] Unlike the MLAT system, which requires separate agreements with each country, the Budapest Convention provides a multilateral framework for cooperation among all signatories. India's non-participation in the Budapest Convention limits its ability to

[65] Diarmaid Harkin et al., *The Challenges Facing Specialist Police Cyber-Crime Units: An Empirical Analysis*, 19 Police Practice and Research: An International Journal, 519, 526-527 (2018).
[66] Directive 2014/41/EU of the European Parliament and of the Council regarding the European Investigation Order in criminal matters (2014) OJ L130/1, art 1(1).
[67] Convention on Cybercrime art. 16, Nov. 23, 2001, Council of Europe, ETS No. 185.
[68] Convention on Cybercrime art. 17, Nov. 23, 2001, Council of Europe, ETS No. 185.
[69] Convention on Cybercrime art. 20, Nov. 23, 2001, Council of Europe, ETS No. 185.
[70] Convention on Cybercrime art. 35, Nov. 23, 2001, Council of Europe, ETS No. 185.

benefit from these more efficient mechanisms for international cooperation in cybercrime investigations.

The United States has implemented the CLOUD Act, which provides a framework for bilateral agreements that allows law enforcement agencies to request electronic data from partner countries directly, bypassing the often lengthy MLAT process.[71] This approach significantly expedites cross-border data access for cybercrime investigations compared to the Indian framework, whose heavy reliance on the traditional MLAT process is lower and less efficient in accessing electronic data from foreign service providers.

Australia's Telecommunications and Other Legislation Amendment (Assistance and Access) Act 2018 provides law enforcement agencies with enhanced powers to access encrypted communications in certain situations, aiming to tackle the growing challenge of encryption in cybercrime investigations.[72] India lacks specific legislation that provides clear powers for accessing encrypted communications, which can hamper investigations involving encrypted data and communications, making it harder to track cybercriminals.

5. Recommendations

The jurisdictional challenges in addressing cross-border cybercrimes require a multi-faceted approach combining domestic legislative reforms with international cooperation. While Indian courts have shown remarkable flexibility in interpreting existing provisions to address cybercrimes, legislative intervention may be necessary to resolve current anomalies and provide more precise guidance.

The success of any legal framework in addressing these challenges depends not only on comprehensive domestic legislation but also on international cooperation and harmonisation of laws. As technology continues to evolve, the legal framework must maintain a delicate balance between territorial sovereignty and the borderless nature of cyberspace. While providing a foundation for addressing cybercrimes, the current framework requires continuous adaptation to meet emerging challenges in this rapidly evolving domain.

[71] Clarifying Lawful Overseas Use of Data Act, Pub. L. No. 115-141, div. V, § 103, 132 Stat. 1213, 1224 (2018).
[72] Telecommunications and Other Legislation Amendment (Assistance and Access) Act 2018 (Cth) pt 15 (amending Telecommunications Act 1997 (Cth)).

On the other facet, India has made notable progress in building a framework for investigating and prosecuting cross-border cybercrime. However, there are several areas where the current system's effectiveness could be significantly enhanced. The cross-border nature of these crimes often requires timely access to electronic evidence, cooperation with foreign entities, and the ability to act swiftly to pursue cybercriminals operating beyond national borders. Potential areas for development include:

(i) Exploring participation in international conventions like the Budapest Convention to access more efficient mechanisms for international cooperation.

(ii) Investing in specialised cybercrime units and continuous training programs for law enforcement personnel to bridge the skills gap in handling complex, cross-border cases.

(iii) Developing expedited processes for data sharing and evidence collection in cybercrime cases, possibly through bilateral agreements similar to the US CLOUD Act.

(iv) Enhancing legislative frameworks to keep pace with technological advancements, potentially including provisions for accessing encrypted data while balancing privacy concerns.

As the digital landscape continues to evolve, so too must the frameworks and capabilities of law enforcement agencies to effectively combat cross-border cybercrimes. India's approach to this challenge will be crucial in shaping its cybersecurity landscape and its ability to protect its digital assets in an increasingly interconnected world.

6. Conclusion

Advancement in technology and the phenomenon of globalisation have presented new challenges in the field of cybercrime. Unlike traditional crimes it is very crucial to carefully apply the principle of territorial limits as it can directly impact the interests of a state. Similarly, other principles work in an overlapping manner to protect the victims. Indian Judiciary has evolved to include cybercrime within its purview. The concept of cross border crimes in IT Act grants the Indian Court with the power to claim jurisdiction over cross border cybercrimes. BNSS and BNS also extend the jurisdiction of Indian Courts over such cross-border crimes.

However, India despite several efforts, is not a part of Budapest Convention, which hinders

India from gaining several benefits to resolve cybercrimes in a time bound manner with lower chances of offenders running away to safe havens. India relies on bilateral treaties with other states to resolve such offences which can be cumbersome and time consuming depending on the legal requirement of the state.

The government of India has played an active role in developing the mechanism against cross-border cybercrimes, but the investigation procedure is still dependent upon the cooperation with other states. The increase in such offences is alarming and cannot be addressed efficiently through time taking process. Non-coherence between the place where crime is committed and the place where digital infrastructure is located along with the delays and lack of consonance between the laws of states are some of the reasons as to why there is a need to establish an organised framework for resolving cybercrimes across boundaries.

Developing specialised crime units, building capacity and streamlining the laws related to cybercrimes across borders could help India to safeguard the interest of victims thereby setting an example globally.