Jus Corpus Law Journal

Open Access Law Journal – Copyright © 2026 – ISSN 2582-7820

Editor-in-Chief – Prof. (Dr.) Rhishikesh Dave; Publisher – Ayush Pandey

Transnational Cybercrime Jurisdiction under the Bharatiya Nagarik Suraksha Sanhita 2023: Mapping the Gap Between Substantive Reach and Procedural Enforcement

Manya Shah[a]

[a]Jindal Global Law School, Sonipat, India

Received 30 May 2026; *Accepted* 30 June 2026; *Published* 04 July 2026

Cybercrime is often considered naturally transnational: ransomware servers may be located in one country, the victim in another, and the data flows through a third. In recent years, we have seen that India as a nation has adopted the Bhartiya Nagrik Suraksha Sanhita 2023 (BNSS), but still, the territorial assumption regarding the jurisdiction and trial of the case depends upon the Code of Criminal Procedure Act 1973. Various laws, such as the extraterritorial provisions of the IT Act 2000, in the Indian legal system still struggle to have effective provisions that deal with cybercrime that has taken place outside Indian Jurisdiction. In this article, we will map out the jurisdictional void across investigation, trial, and enforcement outcomes against offenders who are abroad. We will also evaluate the procedures of BNSS and address these gaps effectively using these procedures. Our main objective will be to conduct a critical analysis of the matter to formulate a framework combining statutory amendments, treaty accession, and institutional capacity building.

Keywords: *transnational, cybercrime, extraterritorial provisions.*

INTRODUCTION

Cybercrime is indifferent to borders; as we can see, a ransomware attack originating from servers that are located in Eastern Europe is routed through proxy infrastructure in Southeast Asia and strikes the victim in Mumbai within seconds. Massive development seen in technology has made it easy for the offenders to conduct such a crime without being caught. Initially, when the criminal procedure was formulated, it was believed that the crime occurred at a single and identifiable place, and the courts of such a place had jurisdiction to hear such cases. This essay examines whether India's most recent overhaul of criminal procedure, the Bharatiya Nagarik Suraksha Sanhita 2023 ('BNSS'), which replaced the Code of Criminal Procedure 1973 ('CrPC'), has meaningfully addressed this mismatch when read alongside the extraterritorial provisions of the Information Technology Act 2000 ('IT Act'). We would like to argue the fact that while IT Act covers up the offences committed by computer system that are present within India while on the other hand BNSS that has various sections that are adopted form CRPC which depends upon the jurisdiction of the offence within India which leaves a major gap in our system regarding what India can claim to try lawfully and what sort of investigation evidence and enforcement India could do.

We would like to provide this analysis by explaining it through five parts. Part II examines the extraterritorial reach asserted by section 75 of the IT Act. Part III turns to the territorial jurisdiction provisions of the BNSS and asks whether they have been adapted for cyber-offences. Part IV addresses the evidentiary bottleneck created by cross-border data flows. Part V, we will consider the mutual legal assistance and extradition framework, taking a comparison with the Budapest Convention as a comparative benchmark. Finally, in Part VI, we will be focusing on a set of reforms that we could implement and end with a conclusion.

SUBSTANTIVE REACH: SECTION 75 OF THE INFORMATION TECHNOLOGY ACT 2000

Section 1(2) of the IT Act applies to any offence or contravention that is committed outside India by any person.[1] Section 75 is an additional expansion to this section, which applies to an offence or contravention committed outside India by any person, irrespective of their nationality, if the act involves the use of a computer, computer system, or computer network

[1] Information Technology Act 2000, s 1(2)

that is located within India. [2]This puts a limitation on transnational crime that is done outside India. This also puts a restriction on the ability to trace the source of crime. Though it is not limited by nationality and the trigger is a computer source that is supposed to be located within India, which covers a major amount of crime that is done within the jurisdiction of India, hence it will serve those victims that affected by cybercriminals within India. The conceptual difficulty is not with the breadth of the assertion, but it is the enforceability. Jurisdiction is seen as a sense of prescriptive authority in which the Indian Parliament has the power to declare an act to be an offence, and no other international law has the power to question such a declaration. There is a territorial nexus that exists.[3] Jurisdiction in the sense of enforcement authority focuses on the power to compel the attendance of an accused, search premises, or seize evidence, which cannot be done without the consent of the state in which the accused or the evidence has been located be exercised extraterritorially. Section 75 (2) preserves the difference by leaving enforcement to be governed by the ordinary procedure of law,[4] which is derived from the BNSS.

The result is similar in transnational criminal law, which allows the state to declare an expansive jurisdictional reach of substantive law while its procedural code remains silent on how that is to be operationalised against persons and evidence located abroad. Various Annual reports have suggested the massive increase in cyber offenders who are present outside India, which shows the current procedural gap in our system. In the following section, we will understand these procedural gaps that are still persistent in our system.[5]

TERRITORIAL JURISDICTION OF COURTS UNDER THE BNSS 2023

The BNSS has reorganised and renumbered sections of the CrPC, which its drafters have described as a comprehensive modernisation of criminal procedure. Yet on the specific question of where a criminal court may try an offence, the BNSS reproduces the provisions that are present in the CrPC approach. Sections 197 to 199 of the BNSS, which govern the place of inquiry or trial, track sections 177 to 179 of the CrPC almost verbatim.[6] An offence is ordinarily to be tried by a court within whose local jurisdiction it was committed, with

[2] Information Technology Act 2000, s 75
[3] Susan W Brenner, 'Cybercrime Jurisdiction' (2006) 46 Crime, Law and Social Change <https://doi.org/10.1007/s10611-007-9063-7> accessed 25 May 2026
[4] Information Technology Act 2000, s 75(2)
[5] Ministry of Home Affairs, *Annual Report 2023–24* (Indian Cybercrime Coordination Centre (I4C), 2024)
[6] Code of Criminal Procedure 1973, ss 177, 178 and 179

limited extensions for offences committed partly in one local area and partly in another, or for an offence consisting of several acts done in different local areas and partly in another, or for offences consisting of several acts done in different local areas.

For a cyber-offence, this framework raises questions that the BNSS does not directly answer. Where a phishing email is composed on a server in one country, transmitted through intermediary servers in several others, and opens a fraudulent webpage that deceives a victim in India, at what point has the 'offence' been 'committed' for sections 197 to 199?[7] The BNSS, like the CrPC before it, does not contain a cyber-specific deeming provision that would locate such an offence at the place where its consequence is felt, as opposed to the place where the constituent act occurred. In practice, Indian courts have tended to assume jurisdiction wherever a consequence of the offence is experienced, an approach consistent with the broad language of section 75[8] of the IT Act, but this is achieved through judicial extension of general principles rather than through any explicit statutory mechanism in the BNSS itself.

This is a missed legislative opportunity. The BNSS introduced numerous provisions explicitly responsive to electronic processes, for instance, expanded recognition of electronic communication for the service of summons and the recording of statements by audio-video means. Yet none of these provisions addresses the prior and more fundamental question of which court has territorial jurisdiction over an offence whose constituent elements span multiple jurisdictions, whether those jurisdictions are different Indian states or different countries entirely. The absence of a cyber-specific jurisdictional rule in the BNSS means that, for transnational cases, courts continue to rely on the same case-by-case, fact-sensitive determinations that proved cumbersome under the CrPC, with no statutory guidance tailored to the realities of distributed computer networks.

THE EVIDENCE PROBLEM: CROSS-BORDER DATA AND THE BNSS ELECTRONIC EVIDENCE REGIME

Once the territorial jurisdiction of the case is established, the main problem arises when the prosecution is founded on electronic evidence, requiring that the evidence be gathered, authenticated, and produced before the court. The admission of electronic records in India is

[7] Bharatiya Nagarik Suraksha Sanhita 2023, ss 197, 198 and 199
[8] Information Technology Act 2000, s 75

covered by the Bharatiya Sakshya Adhiniyam 2023,[9] which also requires additional amount of authentication of the evidence, which is analogous to the recent case heard in the Supreme Court of India in Arjun Panditrao Khotkar v Kailash Kushanrao Gorantyal.[10] According to section 63 of this Act, there is a requirement for a certificate, which is used to identify the electronic records. This is essential for the authentication of the electronic device. This certificate also includes various particulars of the device involved. Where the device or server in question is located outside India and controlled by a foreign service provider, obtaining such a certificate, let alone the underlying data, depends entirely on the cooperation of that provider or of the foreign state in which it operates.

The BNSS provisions on search, seizure, and production of documents were not drafted keeping this consideration in mind. An order under the BNSS that directs a person to produce a document or electronic record operates and is enforceable only to those who are within the territory of India. So, if we look at a foreign-incorporated platform with no establishment in India, it cannot, as a practical matter, be compelled or forced by an Indian court's order alone to preserve or disclose the data held on its platform servers abroad. Investigators are accordingly left with two possible, imperfect options: a formal method and an informal method. In the informal method, there is a request through the platform's law-enforcement liaison channels, which are voluntary, inconsistent in response time, and offer no judicial oversight. Formal mutual legal assistance requests, addressed in Part V, which are frequently too slow to capture volatile digital evidence before it is overwritten or deleted.

A further complication arises from India's own data protection framework. The Digital Personal Data Protection Act 2023 contains provisions restricting the transfer of personal data to certain jurisdictions.[11] On the other hand, the foreign data protection regimes impose reciprocal restrictions on the export of data to India. Where a cyber-offence investigation requires data that is itself personal data under both the requesting and the responding state's law, an additional layer of legal friction is introduced that neither the BNSS nor the IT Act addresses, and which existing mutual legal assistance frameworks were not designed to resolve efficiently.

[9] Bharatiya Sakshya Adhiniyam 2023
[10] *Arjun Panditrao Khotkar v Kailash Kushanrao Gorantyal & Ors* (2020) 7 SCC 1
[11] Digital Personal Data Protection Act 2023, s 17

MUTUAL LEGAL ASSISTANCE, EXTRADITION, AND THE BUDAPEST CONVENTION

If there is enough evidence that proves that the accused is located outside India. India's primary formal mechanism is the bilateral mutual legal assistance treaty (MLAT), which gives effect through letters rogatory issued under the BNSS. The bilateral model requires a separate treaty and separate institutional relationships with each cooperating state. If we come about and focus on its weaknesses in the cybercrime context, it has a really slow speed, such as gathering digital evidence regarding connection logs, IP addresses, location, and cached content that are only valid for a week or a short period of time. On the other hand, the MLAT request is routed through diplomatic and judicial channels in two states, which routinely take many months to be executed. The Council of Europe's Convention on Cybercrime, commonly known as the Budapest Convention, was designed precisely to address this mismatch. It establishes a multilateral framework requiring signatories to maintain a 24-hour and seven-day-a-week point of contact for urgent assistance. This is done to provide the expedited preservation of stored computer data pending the completion of a formal request.[12] India is not a signatory to the convention. India has historically expressed reservations rooted in concerns about sovereignty, most acutely in relation to Article 32(b), which permits a party to access stored data located in another party's territory with the consent of the person who has lawful authority to disclose it, without requiring the consent of the state in whose territory the data is held.[13] Experts and the general public have given their opinion on this matter, stating that this provision, which aims to improve cooperation with willing private parties, is unsuitable for the traditional conceptions of territorial sovereignty over data control and protection, as this has been a significant obstacle for various states, including India, which is not part of the convention.[14]

Other nations and jurisdictions, on the other hand, have pursued alternative models that may offer more politically palatable templates. The United States of America uses the United States' Clarifying Lawful Overseas Use of Data Act 2018 permits US law enforcement to compel US-based providers to produce data within their custody or control, regardless of

[12] Budapest Convention 2001
[13] Budapest Convention 2001, art 32(b)
[14] Jonathan Clough, 'A World of Difference: The Budapest Convention on Cybercrime and the Challenges of Harmonizations' (2014) 40(3) Monash University Law Review <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2615789> accessed 25 May 2026

where the data is physically stored. This also creates a mechanism for foreign governments meeting baseline human rights standards to enter into a bilateral agreement, which allows direct requests to the service providers.[15] The European Union's e-evidence regulations create an effective framework of European Production Orders, which allows judicial authorities in one member state to compel service providers in another to produce or preserve data directly. This is subject to defined sets of safeguards.[16] This model is effective as it does not require the requesting state to abandon the principle that evidence located abroad is subject to the sovereignty of the state where it is held. Instead, it creates a regulated and judicially supervised channel for direct contact with the intermediaries, but, if we see India, it has yet to be adopted in any statutory form. Our main objective is not merely evidence but the physical presence of an accused. India has recourse to this through the Extradition Act 1962, which defines an 'extradition offence' by reference to dual criminality: conduct that would constitute an offence under the law of both India and the requesting or requested state.[17] Cyber-offence definitions vary considerably across jurisdictions in their constituent elements, thresholds, and even their basic categorisation; conduct treated as a serious computer-fraud offence in one jurisdiction may fall under a lesser data-protection or consumer-law contravention in another. This variance creates a genuine risk that dual criminality, as a threshold requirement, will not be straightforwardly satisfied even where both states criminalise broadly similar underlying conduct, further constraining India's ability to secure the presence of an accused located abroad.

TOWARDS REFORM: A SEQUENCED APPROACH

In the following analysis, we will understand the gap between India's substantive jurisdictional reach and its procedural enforcement capacity, which cannot be closed by a single legislative intervention but requires coordinated reforms across the three levels.

First is that BNSS could be amended, and it can introduce a dedicated chapter which deals with cyber offences jurisdiction and cross-border investigation. Such chapters will be really effective as the provisions will be given clearly, and this will allow courts to make decisions without creating confusion regarding which laws will be applicable. Second, at an

[15] Clarifying Lawful Overseas Use of Data Act 2018, s 2713
[16] Electronic Evidence in Criminal Proceedings 2023
[17] Extradition Act 1962

international level, India should take inspiration from conventions such as the Budapest Convention, which address such situations in depth, like Article 32(b), which has formulated a successful framework that works towards dealing with cybercrime in depth. Third, at the institutional level, the Indian Cybercrime Coordination Centre should be given an expanded mandate and dedicated legal staff to serve as a centralised cyber-MLAT cell, coordinating time-sensitive requests with platform law-enforcement portals and the Ministry of External Affairs. Without such capacity, even well-drafted statutory mechanisms will be underused in practice.

CONCLUSION

The BNSS 2023 has brought about major changes in the system of the country as it has worked towards clarifying various provisions under CrPC, which were not yet covered; still, we observe that provisions regarding cyber law and cybercrime are still unclear, and we often rely on territorial assumptions that are present under CrPC. Section 75 of the IT Act allows India to take cybercrime seriously on paper, but in terms of procedural and diplomatic architecture, it has yet to reach that level. Closing this gap requires legislative amendment of the BNSS itself. A more effective solution could be achieved by working on a cooperation framework and institutional investment.