Page 745 - 750

INTERNATIONAL JOURNAL OF LAW MANAGEMENT & HUMANITIES

[ISSN 2581-5369]

Volume 9 | Issue 4

2026

Cross-Border Cybercrime Investigation under Bharatiya Nyaya Sanhita, 2023 and International Cooperation

DR. SHAMBHU SINGH RATHAUR*

ABSTRACT

Cross-border cybercrime highlights the tension that exists between territorial criminal process and globally dispersed digital evidence. India's Bharatiya Nyaya Sanhita, 2023 (BNS) enlarges the scope of conduct outside India that is considered actionable, including offences committed against computer resources situated in India. However, jurisdiction to legislate is not equivalent to the ability to investigate a crime and collect admissible digital evidence in another jurisdiction. This article discusses the interplay between the BNS, the Bharatiya Nagarik Suraksha Sanhita, 2023 (BNSS), the Bharatiya Sakshya Adhiniyam, 2023 (BSA) and the Information Technology Act, 2000 (IT Act). India's want of capacity in its criminal process to deal with cybercrime lies in procedure and institutions rather than in substance alone: the BNSS provides the basis for letters of request and reciprocal assistance, whereas the BSA strengthens the requirements of certification and integrity. Neither framework, however, caters for the speed at which cloud deletion, encryption and multi-jurisdictional platforms operate. This article recommends a dual, rights-based process of cooperation, that is, preservation and 24/7 coordination ahead of a fast and standardised system of mutual legal assistance.

Keywords: *Bharatiya Nyaya Sanhita, cybercrime, mutual legal assistance, electronic evidence, digital forensics, jurisdiction, international cooperation*

I. INTRODUCTION

Cybercrime is inherently transnational. A fraudster can operate from one jurisdiction, route traffic through several others, use a platform registered in a third place, store the proceeds in a fourth country and attack either an Indian citizen or an Indian computer resource. The first few investigative days can matter more than the subsequent court hearing, because logs are deleted, accounts are closed, cloud data is moved and proceeds are laundered through cryptocurrencies or money mules. India's present-day statistics reveal the scale of the issue. Government data records 19,18,835 cases of financial fraud and a loss of about ₹22,848 crore through the

* Author is the Principal at Sir Pratap Vidhi Mahavidyalaya, Jodhpur, Rajasthan, India.

 [ISSN 2581-5369]

National Cybercrime Reporting Portal in 2024; the 1930 helpline and the Citizen Financial Cyber Fraud Reporting and Management System are designed to stop the flow of funds.[1]

The 2023 criminal law reforms are therefore important, but their impact must be considered in the light of three separate questions: whether India can make its nationals criminally liable; whether Indian authorities can investigate the conduct and gather the evidence; and whether that evidence can then be used in court. The first of these questions can be answered with more certainty than the other two. The BNS expressly covers some extraterritorial conduct, and the IT Act contains an extraterritorial clause. Neither statute, however, permits an investigation outside India's borders.

The present study reveals the same fault line from different perspectives. Studies of UPI fraud focus on rapid transactions, social engineering, the use of money mules and the difference between electronic activity and forensic evidence.[2] In relation to the problem of liability on the dark web, anonymity and attribution, along with the need for international collaboration in law enforcement, have been pointed out.[3] Studies of the Indian criminal law reforms also warn that the newly constructed statutory framework will need harmonisation and judicial interpretation.[4]

II. The BNS: A Wider Reach, Not a Complete Investigative Solution

The BNS does not establish a self-standing "cybercrime code". Cyber-enabled crimes continue to be tried under overlapping provisions of the IT Act and ordinary criminal law. Phishing, digital arrest frauds and fraudulent payment practices may constitute offences of identity theft and personation for cheating under the IT Act, while the BNS supplies the general offences of cheating and personation. Sections 318 and 319 cover deception, inducement and personation, but do not require the medium to be analogue or digital. That is a strength, because the offences are not technology-specific and would not become outdated in the event of any technological advance by criminals.[5]

---

[1] Press Information Bureau, Ministry of Home Affairs, *Cyber Crime: Government Initiatives and Data*, Press Release PRID 2226441 (Feb. 2026).

[2] Shilpa K.L. & Manindra Singh Hanspal, *Investigation of Cyber Frauds in India*, 2(3) Aviradha Int'l J.L. & Legal Stud. (2026), doi:10.65785/aijlls.v2i3.17.

[3] Kriti Singh, Gouri Malhotra & Gaurav Kumar, *Dark Web and Criminal Liability in India*, 7(3) Int'l Res. J. Multidisciplinary Scope 49, 49–58 (2026), doi:10.47857/irjms.2026.v07i03.012119.

[4] Nikhil Naren & Kashish Gupta, *Rethinking India's Cybercrime Law: From Information Technology Act to Emerging Threats in a Global Context*, Int'l Rev. L., Computers & Tech. (2026), doi:10.1080/13600869.2026.2668321; Rahul Kailas Bharati, *The New Criminal Law Paradigm in India and Its Impact on Cybercrime Adjudication* (July 24, 2025), SSRN, abstract no. 5378219.

[5] The Bharatiya Nyaya Sanhita, 2023, No. 45 of 2023, ss. 318–319 (India); Information Technology Act, 2000, No. 21 of 2000, ss. 66C–66D (India).

 [ISSN 2581-5369]

Section 1(5)(c) of the BNS is the key provision extending jurisdiction beyond the borders of India to cover offences targeting a computer resource located in India. Section 1(4) further recognises offences committed in foreign countries, provided that there are grounds under Indian law for the prosecution of such acts. Read together with section 75 of the IT Act, these two provisions supply a very solid basis for prescriptive jurisdiction. It means that a foreign individual may be prosecuted for an attack on an Indian bank, online platform, server or other Indian computer resource even though the act was committed abroad at a foreign keyboard.

Two main requirements attach to the BNS. First, a statutory nexus must be proved, meaning that either a computer resource was located in India or some other ground recognised by Indian law supports the assertion of jurisdiction. Second, the difference between the assertion of jurisdiction and the execution of jurisdiction must be kept in mind. India is not entitled to dispatch its police officers to conduct a forensic analysis of a foreign server, to arrest a suspect residing abroad or to seize data held by a provider under the sovereignty of another state.

III. BNSS Investigation and BSA Proof in a Cloud Environment

The BNSS strengthens the language of domestic investigation. Section 94 expressly refers to electronic communications as well as to communication devices that may hold digital evidence. Section 105 requires the recording of search and seizure by audio-visual electronic means. These sections enhance transparency and the chain of custody where a phone, laptop, local server or storage device is seized domestically. The BNSS also devotes an entire chapter to reciprocal arrangements. Sections 110 to 124 deal with foreign service of process, letters of request, the transfer of persons, the attachment or forfeiture of property and the method of transmitting a request between India and a contracting state.[6]

Section 112 is especially significant, since it enables a court to issue a letter of request to a competent authority in another country to conduct an investigation there. Section 123 routes all such letters through the Central Government. This is the only way to obtain subscriber information, transactional records, witness statements, or the results of searches of devices held abroad. It is not, however, an emergency preservation procedure. The Sanhita itself establishes no process for a speedy request to a provider for such information before it is destroyed.

The BSA deals with the next step. Section 61 gives an electronic or digital record the same force and effect as a paper document, subject to section 63. Section 63 still contains conditions about the computer or communication device, habitual use, lawful possession and the manner in which the output was produced. This does not mean that everything printed out or downloaded

[6] The Bharatiya Nagarik Suraksha Sanhita, 2023, No. 46 of 2023, ss. 94, 105, 112, 123 (India).

 [ISSN 2581-5369]

becomes inadmissible evidence; what it requires is that the form in which the evidence exists be identified, that the original or best evidence be preserved, that its extraction be demonstrated and that a proper certificate be obtained.[7]

Supreme Court jurisprudence on electronic evidence remains very much important. In *Anvar P.V. v. P.K. Basheer*, the Supreme Court treated statutory certification as the primary mode of admitting secondary electronic evidence.[8] In *Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal*, the Supreme Court reiterated the relevance of certification but made it clear that there is a difference between an original electronic record and a copy of it.[9] Under the BSA, law enforcement agencies must consider admissibility at the time of collecting foreign evidence, and not once that evidence has been translated into English in India.

Three additional risks attend the collection of evidence across borders. First, there is a question of authenticity, as a foreign provider must be able to provide a reliable explanation of the system, the account, the time zone and the process by which the information was extracted. Second, there is an issue of continuity: there must be an intelligible chain linking the request, production, hashing, transmission, storage and examination of the record. Third, there is a problem of proportionality: a cloud account may store much more data than is relevant to the alleged crime. The privacy right established by *K.S. Puttaswamy (Retd.) v. Union of India* requires a legal basis, necessity and measures protecting against overbroad access.[10]

IV. International Cooperation: From MLAT Delay to Operational Coordination

India's current international structure is multi-layered in nature. The Ministry of Home Affairs has jurisdiction over mutual legal assistance in criminal matters, while the Ministry of External Affairs maintains a list of 39 MLATs or agreements currently in force. Depending on the text of the treaty, these instruments have been used to facilitate the service of documents, the collection of evidence, search and seizure, the transfer of exhibits, the identification of persons and objects, and the restraint or confiscation of proceeds. It should be noted that, in the cybercrime context, the main limitation of the treaties relates not to their legal form but to the factors considered below.[11]

---

[7] The Bharatiya Sakshya Adhiniyam, 2023, No. 47 of 2023, ss. 61–63 (India); Devansh Malhotra & Rohit Kumar Shrivastava, *Bytes and Rights: Unpacking Search and Seizure of Electronic Evidence Under India's Legal Framework*, 4(1) NFSU J. Forensic Just. (2025), doi:10.62995/jfj9820251028.

[8] *Anvar P.V. v. P.K. Basheer*, (2014) 10 SCC 473 (India).

[9] *Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal*, (2020) 7 SCC 1 (India).

[10] *K.S. Puttaswamy (Retd.) v. Union of India*, (2017) 10 SCC 1 (India).

[11] Ministry of External Affairs, Government of India, *Mutual Legal Assistance in Criminal Matters* (Apr. 3, 2026).

 [ISSN 2581-5369]

The Budapest Convention is the most advanced framework treaty on cybercrime cooperation, because it combines substantive provisions with fast-track preservation and procedure as well as a 24/7 network. India has not acceded to this Convention, though it is part of the G7 24/7 contact point network. Non-adherence does not bar India from adopting the practices contained in the framework treaty. It simply means that Indian investigating agencies cannot rely on the treaty-based preservation and cooperation mechanisms of the Convention with countries that reserve them for parties alone.[12]

The United Nations Convention against Cybercrime expands the diplomatic possibilities. This Convention was adopted by the General Assembly in Resolution 79/243 on 24 December 2024.[13] It became open for signature in October 2025 but is not yet in force; according to the United Nations Treaty Collection, as at 9 July 2026 there were 78 signatures and three parties to the Convention.[14] India was not one of the signatories on that status page. What makes the Convention valuable for India is its global perspective and its focus on cooperation, evidence, and technical and capacity-building assistance. The risks associated with the Convention are also significant: wide cooperation powers should not weaken legality, privacy, data protection and the rights of the accused.

The practical solution would consist of two parallel tracks. The first track would entail immediate preservation and operational coordination. An I4C expert, or a 24/7 cell staffed by one, would receive a time-sensitive request, identify the provider and the jurisdiction involved, issue or arrange for the issue of a preservation request to the extent allowed by law, freeze domestically derived proceeds using the existing financial system, and guide the investigating officer on the correct route to go abroad. The second track would entail the official BNSS and MLAT process, launched immediately with the help of a standardised, translated and narrowly drafted letter of request.

V. A Reform Agenda for India

The four reforms may be enumerated as follows. First, India must formulate a BNSS request protocol for cybercrime, specifying standard formats for preservation, subscriber, traffic and content data, cloud imaging and asset restraint orders.

[12] Council of Europe, *India, Octopus Cybercrime Community* (last visited July 14, 2026).
[13] G.A. Res. 79/243, annex, *United Nations Convention Against Cybercrime: Strengthening International Cooperation for Combating Certain Crimes Committed by Means of Information and Communications Technology Systems and for Sharing of Evidence in Electronic Form of Serious Crimes* (Dec. 24, 2024).
[14] U.N. Treaty Collection, *United Nations Convention Against Cybercrime*, status as of July 9, 2026.

 [ISSN 2581-5369]

Second, there is an urgent need for an I4C-led, integrated case management system for cyber investigations. The existing cybercrime reporting portal and suspect identifier repository are quite useful for quick triage, but complaint information is not evidence of criminality. Investigative analytics should not be confused with evidentiary findings, and audit trails and access control mechanisms are essential.[15]

Third, India should develop a national digital forensics standard based on the principles of forensic integrity, privacy minimisation and reproducibility. This standard should include the use of validated tools, write blocking where applicable, hash validation, time zone correction, contemporaneous documentation and a certification process that fits within section 63 of the BSA. Unusually invasive international requests also need judicial authorisation.

Fourth, India should make a public decision on its approach to treaties. Becoming a party to the Budapest Convention or the UN Convention, once suitable safeguards and rules for implementation are put in place, would increase interoperability, but it would also have to be accompanied by domestic rules of necessity, proportionality, dual criminality where applicable, refusal criteria, defence disclosure and remedies for any unauthorised collection. The goal here is not maximal access but reliable and lawful access.

VI. Conclusion

While the BNS makes it easier for India to bring cybercrime cases concerning India, this measure alone cannot solve the problem of territoriality in investigations. The crucial changes will be realised through the practical application of the BNS in combination with letters of request under the BNSS, evidence integrity measures under the BSA, rapid preservation and treaties on cooperation. India needs to change its approach from a file-transmission approach to an operational approach, whereby the process of preservation starts immediately and is followed by formal assistance in a controlled and rights-compliant way. For the BNS to work in cases of cybercrime, substantive jurisdiction, investigative jurisdiction, international cooperation and evidence reliability need to work as one whole.

*****

[15] Ministry of Home Affairs, Government of India, Lok Sabha Unstarred Question No. 2729 (Dec. 16, 2025); Sanskriti Pathak, *Cyber Crimes in India and Challenges for Investigation Agencies* (Feb.–Mar. 2026), SSRN, abstract no. 6907898.

 [ISSN 2581-5369]