INDIAN JOURNAL OF LEGAL REVIEW [IJLR – IF SCORE – 7.58]

VOLUME 6 AND ISSUE 4 OF 2026

APIS – 3920 - 0001 *(and)* ISSN - 2583-2344

Published by

Institute of Legal Education

https://iledu.in

NAVIGATING THE DIGITAL BORDER: A COMPARATIVE ANALYSIS OF CROSS-JURISDICTIONAL HURDLES IN INDIA'S TRANSNATIONAL CYBERCRIME INVESTIGATIONS

AUTHOR – MANVENDRA SINGH* & MANEESH ADESH SRIVASTAVA**

* 2ND YEAR L.L.M. STUDENT AT RAMA UNIVERSITY, KANPUR

** ASSISTANT PROFESSOR, FACULTY OF JURIDICAL SCIENCES, RAMA UNIVERSITY, KANPUR.

BEST CITATION – MANVENDRA SINGH & MANEESH ADESH SRIVASTAVA, NAVIGATING THE DIGITAL BORDER: A COMPARATIVE ANALYSIS OF CROSS-JURISDICTIONAL HURDLES IN INDIA'S TRANSNATIONAL CYBERCRIME INVESTIGATIONS, *INDIAN JOURNAL OF LEGAL REVIEW (IJLR),* 6 (4) OF 2026, PG. 817-828, APIS – 3920 – 0001 & ISSN - 2583-2344.

Abstract

The digital technologies have been embraced exponentially, which has permanently transformed the environment of transnational crime, making the traditional Westphalian concept of territorial sovereignty more of a relic of the past. This research report is a comprehensive, doctrinal and comparative study of the cross-jurisdictional challenges bedeviling the law enforcement agencies in India when investigating and adjudicating transnational cybercrimes. This research helps to unravel the bewildering jurisdictional morass in contemporary digital investigations by critically analysing the very complicated interaction between the domestic legal systems of India, namely, the Information Technology Act, 2000, and the recent introduction of the Bharatiya Nagarik Suraksha Sanhita, 2023, and the procedural requirements of the latter. The approach is mixed, a mixture of doctrinal and comparative, contrasting the Indian legal stance on the issue with the world standards, including the Clarifying Lawful Overseas Use of Data (CLOUD) Act of the United States, the General Data Protection Regulation (GDPR) of the European Union, and the new United Nations Convention against Cybercrime of December 2024.

The results indicate that there is a clear epistemic tension between anarchic cyber criminality and territorially specific police. The existing cross-border digital evidence gathering methods, which are mainly Mutual Legal Assistance Treaties (MLATs), are structurally flawed and lack adequate bureaucratic momentum and legal inconsistency, including the notions of dual criminality and probable cause. The discussion shows that although the statutory framework in India is highly aggressive in asserting extraterritorial jurisdiction based on unilateral long-arm jurisdiction, the application of the law is still stalled by foreign blocking laws and complicated data localization requirements. In the end, the paper will conclude that the solution to such investigative bottlenecks is to ensure that India progresses to a stage of not relying on archaic MLAT, but rather negotiating bilateral executive agreements under the CLOUD Act and aligning its judicial oversight mechanisms with its Section 94 of the Bharatiya Nagarik Suraksha Sanhita, 2023, as well as a proactive manner of directing the norm-setting path of the newly formed UN Cybercrime Convention to ensure the protection of both digital sovereignty and fundamental rights.

Keywords

Digital Sovereignty, Transnational Cybercrime, Extraterritorial Jurisdiction, Bharatiya Nyaya Sanhita, CLOUD Act.

INDIAN JOURNAL OF LEGAL REVIEW [IJLR – IF SCORE – 7.58]

VOLUME 6 AND ISSUE 4 OF 2026

APIS – 3920 - 0001 *(and)* ISSN - 2583-2344

Published by

Institute of Legal Education

https://iledu.in

I. Introduction

The architectural underpinning of the internet was created in such a way that it emphasized survivability, flexibility and the frictionless movement of information over a decentralized global network. By any architectural yardstick or historical insight, it was not, at any rate, intended to accommodate the inflexible territorial borders of the modern nation-state. Thus, the World Wide Web has created a virtual landscape in which geographical space is erased and geographical boundaries are completely undetected by the stream of data packets. This non-geographic cyberspace has simultaneously spawned an entirely advanced generation of transnational cybercriminals that exploit the territorial schism between sovereign nations to commit fraud, cyber-terrorism, data theft, and espionage almost with impunity. When a victim located in New Delhi is defrauded in a sophisticated phishing scheme organized by a criminal syndicate based in Eastern Europe leveraging server infrastructure based in the United States and communication paths by proxies in Southeast Asia, the resulting investigation is catapulted into a crippling conflict of jurisdiction.

The enforcement of the law as traditionally understood by the international law is territorial. The jurisdiction of a police officer usually dissolves when crossing the national border, but the digital evidence that can be used to convict a cyber criminal in the modern world is nearly globalized. India, with one of the largest and fastest growing internet users in the world, is right at the centre of this crisis in the modern criminal jurisprudence. The Indian state has made efforts to expand its jurisdictional boundaries aggressively by domestic laws by claiming extraterritorial jurisdiction on any cyber offence that results in a computer resource falling within its physical territory. But to claim jurisdiction on paper and to actually exercise the jurisdiction in practice are two entirely different things--a fact with which Indian investigators have to deal day in day out. When Indian law enforcement agencies request crucial electronic data, e.g. subscriber information, metadata, or encryption messages content, they soon find out that the information is stored in foreign clouds under foreign privacy regulations. The current international framework of sharing such evidence is based mainly on Mutual Legal Assistance Treaties. A regime that is theoretically pre-digital, as a means of exchanging physical evidence and extraditing fugitives, is clearly straining under the sheer mass and speed of new digital information demands. These treaties are infamous in their snail pace where a single request can take months or even years to process, and by the time the very volatile digital evidence has been overwritten, heavily encrypted, or destroyed permanently.

The new publication of the Bharatiya Nyaya Sanhita, 2023,, and the Bharatiya Nagarik Suraksha Sanhita, 2023, can be seen as a watershed moment in the criminal justice system in India, as these are attempts to modernise the archaic processes, and to directly embed the electronic collection of evidence into the statutes. At the same time, the international community is at a very critical geopolitical crossroad with the signing of a landmark treaty, the United Nations Convention against Cybercrime, in late 2024, which aims to harmonize international cooperation, but falls under the hot debate on digital sovereignty and human rights. It is against this context, which is very dynamic and is changing very fast, that this research aims to unravel the procedural, legal, and diplomatic challenges that hinder the ability of India to effectively police the digital border.

A. Research questions

i. How do the overlapping extraterritorial jurisdictional claims under Section 75 of the Information Technology Act, 2000, and Section 1(5) of the newly enacted Bharatiya Nyaya Sanhita, 2023, impact the substantive prosecution and adjudication of transnational cyber

offences within Indian courts?

ii. To what extent do existing Mutual Legal Assistance Treaties and foreign blocking statutes specifically the United States' Electronic Communications Privacy Act and the European Union's General Data Protection Regulation—structurally obstruct the timely acquisition and admissibility of digital evidence required by Indian law enforcement?

iii. Can modern bilateral mechanisms like the US CLOUD Act executive agreements, or the newly established multilateral frameworks under the 2024 UN Cybercrime Convention, successfully resolve this jurisdictional impasse while maintaining the requisite judicial oversight under the Bharatiya Nagarik Suraksha Sanhita, 2023?

B. Hypothesis

The prevailing reliance on archaic mutual legal assistance mechanisms and unilateral long-arm statutory provisions is fundamentally and structurally inadequate for the unprecedented speed and volatility of transnational cybercrime investigations. It is hypothesized that India cannot effectively overcome cross-border evidentiary hurdles without fundamentally shifting from diplomatic treaty-based requests to direct, law-enforcement-to-provider data sharing mechanisms, a transition that strictly requires the harmonization of domestic judicial oversight under Section 94 of the Bharatiya Nagarik Suraksha Sanhita, 2023, to meet international privacy standards and leverage the frameworks established by the newly adopted UN Cybercrime Convention.

C. Research Objectives

i. To critically analyse the doctrinal foundations and legislative frameworks governing extraterritorial cyber jurisdiction in India, tracing the legal evolution from the Information Technology Act, 2000, to the comprehensive overhaul represented by the new criminal codes.

ii. To evaluate the specific procedural and administrative bottlenecks inherent in cross-border digital evidence collection by exhaustively comparing the Mutual Legal Assistance Treaty regime with alternative comparative models like the US CLOUD Act and the European Investigation Order.

iii. To formulate concrete policy and legal reform suggestions that align India's domestic investigative procedures with emerging global norms, ensuring effective transnational cooperation without compromising the nation's digital sovereignty or the fundamental privacy rights of its citizens.

D. Literature Review

The scholarly debate about jurisdiction of transnational cybercrime has developed substantially within the last two decades, moving beyond initial, somewhat idealistic conceptions of cyber- exceptionalism, which held that cyberspace was a separate sovereign space that could not be governed by laws of land, to highly complicated, practical discussions of digital sovereignty and the clash of laws. The groundbreaking work by Wall defined cybercrime as a dynamic conceptual category, which involves not only the new digital mediums of perpetrating traditional crimes but also the completely new crimes against computer networks themselves. This duality in nature makes the jurisdictional studies incredibly difficult because the locus delicti, the physical location of the crime committed, is now hopelessly divided between the various sovereign states and cloud servers.

The structural paralysis of the Mutual Legal Assistance Treaty regime has been widely reported in the existing legal scholarship. In their detailed blueprint of data sharing between India and the US, Swire, Kennedy-Mayo, Srinivasan, and Srikumar have extensively emphasized the painfully slow and tedious nature of the MLAT process, which consumes an average of ten to forty months before it produces actionable intelligence to the Indian

investigators. The authors also found out two fundamental bottlenecks that afflict Indian law enforcement: the volume of data request generated by the huge number of internet users in India is unprecedented, and the US Electronic Communications Privacy Act requires a demonstration of probable cause before American technology companies can reveal the content of communications to foreign agencies.

The Budapest Convention on Cybercrime of 2001 has been celebrated by Western academics as the gold standard in transnational cooperation in the field of international legal harmonization since the dawn of time. Nonetheless, observers such as Seger and other geopolitical experts have cast a lot of doubt on the inability of India to ratify the treaty over the decades. According to the scholarly opinion, the Indian reluctance is mainly based on the indifference of the country toward the issue of sovereignty, namely, the Articles 32b of the Convention, which allows foreign law enforcement agencies to gain access to the data stored in India without any prior notice or consent of the Indian government.

The current literature on the synthesis of the brand-new criminal code in India, the Bharatiya Nyaya Sanhita and the Bharatiya Nagarik Suraksha Sanhita, exhibits a profound lacuna regarding recent, paradigm-shifting international developments that have taken place as recently as late 2024. Although other studies, such as those by Atrey and Ali have examined the substantive inadequacies of the Information Technology Act, 2000, there is an apparent vacuum of a more doctrinal analysis concerning the interaction of the new search and seizure provisions under Section 94 of the BNSS with the strict judicial oversight requirements of the modern international agreements such as the US CLOUD Act. Moreover, the fact that the United Nations General Assembly has officially adopted the first-ever global UN Convention against Cybercrime in December 2024 makes the previous academic literature on studying global cyber diplomacy suddenly obsolete. This study fills this major epistemic gap by offering a comprehensive study on the nexus between the Indian reformed criminal procedure, the current clash of laws on data protection, and the new geopolitical reality that the 2024 UN treaty has created.

E. Research Methodology

The report is a rigorous mixed-methodological work, which harmoniously combines doctrinal, comparative, and empirical analysis to provide comprehensive and legally valid information. The doctrinal approach is the basic foundation of the study, which entails a granular, textual analysis of primary legal statutes, , including the Information Technology Act, 2000, Act No. 21, Acts of Parliament (India); the Bharatiya Nyaya Sanhita, 2023, Act No. 45, Acts of Parliament (India); the Bharatiya Nagarik Suraksha Sanhita, 2023, Act No. 46, Acts of Parliament (India); and the Digital Personal Data Protection Act, 2023, Act No. 22, Acts of Parliament (India). This legal examination is complemented with a careful examination of historic judicial rulings of the Supreme Court of India and other High Courts that define the limits of extraterritoriality and admissibility of electronic evidence.

The comparative methodology is being actively employed to compare the legal system in India with the existing international models. The paper comparatively evaluates the mutual legal assistance regime and the more specific mechanics of the Clarifying Lawful Overseas Use of Data Act, the European Investigation Order, and the highly procedural prerequisites of the EU General Data Protection Regulation. Moreover, the study has got empirical and case study aspects because it uses secondary data collected through ongoing law enforcement activities. Particularly, it examines the cybercrime investigation statistics and technological interventions including the Trinetra-2 artificial intelligence system, which is currently used by the Uttar Pradesh Police to indicate the practical tension between local technological competencies and international legal barriers. Data sources will be journal

articles, official texts of treaties of the United Nations, government press releases, and legal blueprints prepared by international policy think tanks.

II. The Doctrinal Foundations of Extraterritorial Cyber Jurisdiction in India

The underlying issue of prosecuting transnational cybercrime is deeply rooted in the old law of the land which states that the laws of a sovereign are limited to its strictly defined geographical limits in its territorial jurisdiction only. Nevertheless, the customary international law acknowledges a number of specific principles according to which a state can legitimately claim extraterritorial jurisdiction in an offence. These are the Nationality Principle, which is based on citizenship of the offender; the Passive Personality Principle, which is based on the citizenship of the victim; the Protective Principle, which is based on crimes that threaten the vital national security of the state; and the Effects Doctrine, which is a doctrine of jurisdiction of crimes that are committed entirely abroad but have direct and substantial economic or social effect in the state.[1653]

The statutory reaction of India to the borderless character of the cybercrime is based on the very aggressive interpretation of the Effects Doctrine[1654].. Section 75 of the Information Technology Act, 2000 is the main legislative instrument in this assertion. Section 75(1) provides a broad long-arm jurisdiction that says without any doubt that the provisions of the Act shall be applicable to any offence or contravention committed in any other country by any person regardless of his nationality. To support this incredibly broad assertion by the international norms, the crucial element is given in Section 75(2): the act or conduct that is the offence must relate to a computer, computer system or computer network in India. Such a legislative formulation implies that when a bad actor located in Saint Petersburg uses a global botnet to mount a DDoS attack on a banking server that is physically located in Mumbai, the Indian courts have the hypothetical, statutory authority to prosecute the Russian national.

The concept of extraterritoriality is further embedded in the general penal law directly with the recent, historic reorganization of the Indian criminal justice system, the Bharatiya Nyaya Sanhita, 2023, which entirely replaced the archaic Indian Penal Code of 1860. Section 1(5) of the BNS[1655] adds greatly to the classical principles of jurisdiction, that the Sanhita is applicable to the offences committed by Indian citizens in any place outside and inside India, any person in any ship or aircraft registered in India wherever it is, and most importantly, any person in any place outside and inside India, committing an offence against a computer resource located in India.

The faint change in the wording of the legislation between the phrase in the IT Act that includes the word computer and the phrase in the BNS that includes the term computer resource is far-reaching. It shifts the emphasis of the incidental routing of data through an Indian server to a directed attack on the Indian digital infrastructure. Although these provisions give an impression of domestic sovereignty, they cause serious internal statutory overlaps that haunt prosecutors. An individual cross-border ransomware attack now concurrently results in liabilities pursuant to the IT Act[1656] including Section 43 dealing with damage to computer systems or Section 66 dealing with computer related offences and the BNS Section 303 dealing with data theft or Section 318 dealing with cheating.

III. Substantive Legal Conflicts Between the IT Act, 2000 and the Bharatiya Nyaya Sanhita, 2023

This variety of overlapping statutory charges frequently raises serious constitutional issues

[1653] Susan W. Brenner & Joseph J. Schwerha IV, *Transnational Evidence Gathering and Local Prosecution of International Cybercrime*, 20 J. MARSHALL J. COMPUTER & INFO. L. 347, 350 (2002).
[1654] Information Technology Act, 2000, No. 21, Acts of Parliament, 2000 (India).
[1655] Bharatiya Nyaya Sanhita, 2023, No. 45, Acts of Parliament, 2023 (India).
[1656] Information Technology Act, 2000, No. 21, Acts of Parliament, 2000 (India).

about the concept of the principle of double jeopardy. Art. 20(2), INDIA CONST. art. 20, cl. 2, [1657]expressly states that no individual shall be tried and sentenced on the same offence twice. The increasing trend of law enforcement agencies applying the general criminal provisions in addition to the specific provisions of the IT Act to the same set of facts, has been critically noted by the Bombay High Court and the Gujarat High Court. The courts have on numerous occasions observed that this custom is prejudicial in its manner of making the process of bailing a complicated affair and prolongs the pre-trial litigation in an unwarranted manner.

In common law enforcement, it is common practice among investigating officers to cumulatively apply non-bailable BNS charges on top of bailable IT Act charges as a mere tactic to deny the accused bail. As an example, the offences in the IT Act, Section 66, are usually compoundable and bailable, with relatively less severe penalties. By stark contrast, general cheating under Section 318 of the BNS is not bailable and is punishable by harsh punishment such as imprisonment that may be up to seven years. Such tactical piling clouds the waters of prosecution greatly where the state is required to compose complicated extradition requests to other countries. Extradition treaties are highly based on concept of dual criminality whereby precise and unambiguous mapping of the purported offence to the host country laws is required. A request that includes a convoluted set of general penal code offences and specific cyber law offences against a single act of digital conduct is often deemed by foreign courts to be legally incoherent, so as to cause long delays or even be rejected.

A comparative statutory analysis clearly delineates the distinct operational spheres and overlapping liabilities of these two jurisdictional frameworks. Section 75 of the Information Technology Act, 2000, maintains a primary legislative focus on cyber-specific contraventions, requiring an extraterritorial nexus where the act merely involves a computer or network located in India, and typically prescribes generally bailable penalties for specialized technical offences. Conversely, Section 1(5) of the Bharatiya Nyaya Sanhita, 2023, governs general criminal offences with a subtly different nexus requirement, necessitating that the offender was actively targeting a computer resource located in India. This subtle semantic difference consequently triggers broader criminal liability that is often non-bailable, creating a much harsher penal environment for the accused.

The conceptual depth of the Indian laws should always be aligned with the judiciary interpretation in very practical and cross-border situations. The Supreme Court of India has always understood the logistical difficulties of transnational litigation, and in many cases have put more importance on the sovereign interests of the victim state than the procedural convenience of the foreign offender. In *Om Hemrajani v. State of U.P.*, (2005) a landmark interpretation of cross-border criminal procedure took place. In this case, a financial institution based in Dubai had filed a criminal complaint against the petitioner who had secured huge loans in the United Arab Emirates and later absconded to India where he settled in Ghaziabad, Uttar Pradesh. The extraterritorial crime was cognized by the local Magistrate who issued non-bailable warrants. The legal issue of concern was the interpretation of the meaning of Section 188 of the old Code of Criminal Procedure, now identical to Section 208 of the BNSS, 2023, which is the interpretation of the term at which he may be found. The Supreme Court made a resounding decision that the court in which the complaint is filed and in which the accused is taken voluntarily or involuntarily is the competent court in law. The Court set a very important, lasting precedent that transnational crimes must be judged by determining the convenience of the accused

[1657] INDIA CONST. art. 20, cl. 2.

INDIAN JOURNAL OF LEGAL REVIEW [IJLR – IF SCORE – 7.58]
VOLUME 6 AND ISSUE 4 OF 2026
APIS – 3920 - 0001 *(and)* ISSN - 2583-2344
Published by
Institute of Legal Education
https://iledu.in

against the convenience of the victim, and that the latter must prevail at all costs.[1658]

IV. Procedural Paralysis: Mutual Legal Assistance Treaties and Cross-Border Evidence Collection

Although the jurisprudence in Om Hemrajani lays down a domestic foundation to prosecute the culprits after they are literally on the Indian soil, it does not in any way address the much more widespread issue of obtaining digital evidence or the accused in a hostile or unhelpful foreign jurisdiction. Even though the domestic laws are very strong, the point at which an investigation needs data beyond India, the law structure breaks into fragments. The main, conventional channel of transnational data sharing is still the Mutual Legal Assistance Treaty. Today India has MLATs with more than forty countries, formal agreements which are aimed to organize the process of the evidence exchange, freeze bank accounts of illegal bank accounts and carry out the legal orders on the international level.[1659]

Nevertheless, even legal experts and practitioners in law enforcement acknowledge that the MLAT process is inherently flawed in the digital era of the XXI century when cross-border cooperation implies the transfer of physical bank ledgers or the official extradition of a wanted offender. It was not created to record volatile Random-Access Memory data, tracing the short-lived cryptocurrency transactions across decentralized ledgers, or ensuring highly encrypted cloud backups.

In the case of an Indian police officer who is in dire need of the information contained in an email which is stored on the server of a United States-based service provider to stop a current fraud, the officer cannot just email the tech company. The request has to go through a tortuous bureaucratic maze. It has to be sent out of the local police station to the Criminal Investigation Department of the state and then to the Indian Ministry of Home Affairs. The MHA should then officially forward the request to the Office of International Affairs in the US Department of Justice. The request is examined by the DOJ and sent to a US federal prosecutor who is then required to persuade a US federal judge to serve a warrant on the tech company according to the US law. After the data has been secured finally, the whole process works the other way round.

This administrative labyrinth consumes an average of ten months in any part of the world but in the case of Indian requests, delays are systemically opaque and notoriously protracted and may take up to more than three years with an average of forty months. A forty-month delay is fatal to the evidentiary chain, digital evidence is highly volatile, and server logs are automatically deleted or overwritten by corporate retention policies in ninety to one hundred and eighty days.

The practical devastating effect of such bottlenecks is very visible at the state level of law enforcement. The Uttar Pradesh Police Cyber Cell is an interesting real-world empirical case study. The state has just registered an enviable 87.8 percent rate of cybercrime convictions and has successfully frozen more than 325 crores in embezzled funds in the year 2025 alone[1660] through the 1930 national helpline, and quick bank coordination. The introduction of the artificial intelligence-driven Trinetra-2 system by the state, which is expertly combining facial recognition with big data analytics of massive scale, can be seen as an indicator of a huge domestic technological potential. However, even with the modernization of seventy-five special cyber police stations and the training of close to eighteen thousand officers, the police of Uttar Pradesh always state that their efforts encounter an insurmountable jurisdictional barrier the moment when the attackers use foreign cloud servers, encrypted

[1658] Om Hemrajani v. State of U.P., (2005) 1 SCC 617 (India).
[1659] PETER SWIRE ET AL., INDIA-U.S. DATA SHARING FOR LAW ENFORCEMENT: BLUEPRINT FOR REFORMS (2019), https://www.orfonline.org/research/india-u-s-data-sharing-for-law-enforcement-blueprint-for-reforms-55825/.
[1660] Diarmaid Harkin et al., *The Challenges Facing Specialist Police Cyber-Crime Units: An Empirical Analysis*, 19 POLICE PRAC. & RSCH. 519, 522 (2018).

forums of the dark web, or anonymizing VPNs. Local technological genius can never penetrate international legal stalemate.

V. The CLOUD Act and the Extraterritorial Reach of Foreign Blocking Statutes

The collapse of the MLAT regime is not simply a question of inefficiency within the administration; the legal standards are incompatible and even violent. The Electronic Communications Privacy Act of the United States bans the disclosure of the content of communication by the United States-based service providers to any foreign government, unless the request is met with the stringent US Fourth Amendment test of probable cause. Indian state police officers, naturally not having specialized training in US constitutional law, often write evidence requests that do not rise to this high standard and the application is summarily denied by the US DOJ. To put an even further strain on the situation is the principle of dual criminality mentioned above, which is incorporated in nearly all MLATs. When a particular act contravenes an Indian speech rule and is strongly shielded by the US First Amendment, the MLAT request is dead on arrival.

The US has passed the Clarifying Lawful Overseas Use of Data Act in 2018 to avoid the complete stalemate of the MLAT regime altogether. The CLOUD Act is probably the most plausible, short-term solution to the Indian problem of data access. It corrects the Stored Communications Act, forcing US technology firms to generate information irrespective of whether it is stored within or outside the US territory[1661]. More importantly to India, the Act allows the US government to conclude bilateral executive agreements with eligible foreign countries. With such an executive order, an Indian law enforcement agency would be able to issue a legal data request directly to firms such as Google or Meta without going through the outdated MLAT process at all.

Nevertheless, to be eligible to enter into a CLOUD Act agreement, the foreign country must prove that it has strong human rights, that its laws governing data collection are clear, and that its procedures are essential to the implementation of the order. It explicitly states that a foreign request of criminal evidence must be reviewed or supervised by a court, judge, magistrate, or other independent body before the order can be executed.

This is a curious, extremely complicated procedural dilemma facing India. The two routes to force the production of documents or electronic communications are provided in Section 94 of the new Bharatiya Nagarik Suraksha Sanhita, 2023[1662] (previously, Section 91 of the CrPC). To begin with, a policeman can give a written order by his or her own authority. Second, a court can grant a formal court summons. The Indian policing practice of investigating officers currently is based on the administrative powers of officers to request data to tech companies without ever going to a magistrate, a highly established practice that lacks any independent judicial checks whatsoever. In order to have a CLOUD Act agreement, international legal scholars would propose that India may not necessarily have to change its core laws, but instead, it would have to change the way it has been policing. India could graciously comply with the strict stipulation of the CLOUD Act of an independent judicial review by executive directives that all transnational data requests be sent solely through the second route, namely, by obtaining a judicial summons under the BNSS under Section 94.

VI. Conflict of Laws: The EU GDPR vs. India's Digital Personal Data Protection Act, 2023

The high tension of cross-border investigations is further aggravated by the growing balkanization of the laws of data protection on the global level. The introduction of tough

[1661] Diarmaid Harkin et al., *The Challenges Facing Specialist Police Cyber-Crime Units: An Empirical Analysis*, 19 POLICE PRAC. & RSCH. 519, 522 (2018).

[1662] Bharatiya Nagarik Suraksha Sanhita, 2023, No. 46, Acts of Parliament, 2023 (India).

privacy systems has presented a drastic conflict of laws, in which a multinational technology company is torn apart between a legal requirement to generate information to an overseas investigator and a domestic legal ban on the transfer of personal information across borders.

The General Data Protection Regulation of the European Union is an ideal example of such tension. Article 48 of the GDPR expressly makes it clear that a judgment of a court or decision of an administrative authority of a third country which obliges a controller or processor to transfer or disclose personal data can only be recognised or enforced as part of an international agreement, e.g. a Mutual Legal Assistance Treaty. As a result, the European companies are legally, unconditionally prohibited to act on direct unilateral demands of the Indian police made by using the Section 75 of the IT Act. Trying to adhere to the Indian order may impose huge GDPR fines on the European company. In this way, the GDPR[1663] simply re-immerses all international inquiries into the dysfunctional, sluggish MLAT process and effectively abrogates the statutory jurisdiction of India to extend to Europe.

Recently, India has found its way into this complicated regulatory area through the adoption of the Digital Personal Data Protection Act, 2023. In accordance with the historic constitutional ruling in *K.S. Puttaswamy v. Union of India*, (2017), the DPDP Act offers a detailed system of processing digital personal information, [1664]that defined privacy as an inherent fundamental right. Comparative study of the two jurisdictions in terms of doctrinal differences shows that there are some differences in the regulatory philosophy of the two jurisdictions. Whereas the GDPR is very prescriptive, rights-intensive, and technology-neutral, i.e. both digital and physical paper information, the DPDP Act of India is exclusively digital, much more consent-based, and most importantly has much broader exemptions of state instrumentalities and law enforcement agencies.

Delving deeper into their specific regulatory features, the scope of application reveals a fundamental divergence between the two regimes: the European Union's GDPR is comprehensive in its approach, governing all personal data across both digital and physical offline records, whereas India's DPDP Act, 2023, is strictly restricted to governing exclusively digital personal data. Regarding their extraterritorial reach, the GDPR applies broadly to any foreign entities monitoring the behaviour of EU citizens. In contrast, the DPDP Act applies to data processing outside India only if it is directly connected to goods or services offered to data principals located within India. Most critically for transnational investigations, the regimes diverge sharply on the issue of law enforcement access. The GDPR imposes a strict Mutual Legal Assistance Treaty requirement for third-country data requests under Article 48, essentially barring direct data transfers to foreign administrative or judicial authorities without an international agreement in place. Meanwhile, the DPDP Act provides broad, sweeping statutory exemptions that are readily available for state agencies maintaining public order, sovereignty, and security, thereby prioritizing domestic state access over rigid procedural barriers.

Some policymakers have forcefully advanced the idea of the fierce political push toward the localization of data, requiring that the exact copy of the key personal information be stored in the servers, which are physically located on the territory of India as the sure means of overcoming the MLAT bottleneck. The Indian agencies in theory have unhindered, instant access by keeping the data confined to sovereign borders. Nevertheless, as noted by the foremost cybersecurity analysts, the concept of mandatory data localization may have a counter-productive effect on the national cybersecurity resilience. It achieves this by establishing honeypots of data of gigantic

[1663] Council Regulation 2016/679, 2016 O.J. (L 119) 1 (EU) [hereinafter GDPR].
[1664] K.S. Puttaswamy v. Union of India, (2017) 10 SCC 1 (India).

scale, centralized, and concentrated on attracting advanced persistent threats, isolating domestic systems from global threat-intelligence networks and resulting in serious operational conflicts with multinational cloud service providers[1665]. The localization debate is therefore a more basic and unresolved conflict between the geopolitical need to have absolute digital sovereignty and the technicalities of distributed cloud architecture.

VII. Geopolitics, Digital Sovereignty, and the 2024 UN Cybercrime Convention

As a result of the extremely disunited and anarchic nature of the global cyber governance, the international community has been engaged in the last few years in an extremely intense process of negotiating a universal treaty to fill in these jurisdictional gaps. The United Nations General Assembly on December 24, 2024, passed the historic United Nations Convention against Cybercrime, the first legally binding global instrument on cyber issues, G.A. Res. 79/243, United Nations Convention against Cybercrime (Dec. 24, 2024).

Intended to be signed by states in 2025 in Hanoi, the treaty is expected to have a massively positive impact on the international collaboration in the prevention, investigation, and prosecution of cybercrimes by creating standardized, internationally recognized models of electronic evidence sharing. During the negotiations prior to the final text, India was very active and vocal in the Ad Hoc Committee. It was also highly demanding with its own domestic issues, including the express criminalization of negligence in safeguarding sensitive personal data, and the absolute necessity of a worldwide 24/7 network to make international phishing infrastructure inaccessible within a short timeframe. The diplomatic policy of India was strongly affected by its long-standing disillusionment with the MLAT system and saw the UN Convention as a one-off chance to build a multilateral mechanism that would finally circumvent the structural hegemony of Western data custodians.

The introduction of the Convention has however sparked a raging debate over the actual meaning of digital sovereignty and protection of human rights. Digital sovereignty is usually the claim by a state to have absolute, undisputed control over the digital infrastructure, information and online practices on its physical territory. The authoritarian states have promoted a high politics understanding of the digital sovereignty in the UN negotiations, which promotes the wide scope of state control over the internet and criminalizing broad categories of online speech in the ambiguous name of fighting cyber-terrorism.

In contrast, the ultimate text of the UN Convention has been subject to harsh, urgent warnings by international human rights groups. Opponents are even more vehement that the treaty creates incredibly lax privacy protections and facilitated sweeping cross-border legal assistance that can easily be misused by dictatorial regimes to spy on dissidents, investigate journalists and aggressively censor free speech [1666]. Although the text contains nominal safeguards, in Chapter II it states that the implementation has to be in compliance with international human rights law, according to the detractors, the text ends up giving too much power to domestic laws, which in effect justifies the intrusive state surveillance on a global scale.

The new Convention is a very sensitive balancing exercise in the case of India. Being a prosperous democracy with constitutional protections of free speech deeply entrenched in its constitution, India has to walk the fine line of the surveillance-intensive treaty without unwittingly giving domestic power a free hand. At the same time, being a fast-growing country that loses the huge amounts of money in

[1665] Peter Swire & DeBrae Kennedy-Mayo, *Risks to Cybersecurity from Data Localization, Organized by Techniques, Tactics and Procedures*, 11 J. CYBERSECURITY 1 (2024), https://academic.oup.com/cybersecurity/article/10/1/tyae006/7633519.

[1666] G.A. Res. 79/243, United Nations Convention against Cybercrime, U.N. Doc. A/RES/79/243 (Dec. 24, 2024).

transnational cyber fraud, it is in dire need of the efficient evidence-sharing systems that the treaty will provide. The convention is basically trying to combine the strict, geographical ideas of the old criminal law with the flowing, borderless principles of cyberspace- a terribly ambitious project that will push the international diplomatic comity to the utmost limits in the next decade.

VIII. Findings and Suggestions

The overall synthesis of the doctrinal, comparative, and empirical study reveals an endemic, long-standing failure in the existing structure of transnational cybercrime investigations. The overreliance of India on Section 75 of the Information Technology Act and Section 1(5) of the Bharatiya Nyaya Sanhita, 2023 though in theory sound in its claim of territorial sovereignty over foreign offenders, is practically made entirely ineffective by the realities of modern cloud computing and foreign blocking laws such as the GDPR. The mechanism of Mutual Legal Assistance Treaty--theoretically required to uphold diplomatic respect among co-equal sovereigns--has tragically become an administrative maze that simply cannot be compatible with digital evidence, which is of a transient, fast-moving nature.

In order to successfully negotiate the digital border and bring criminals of cybercrime to justice, the following strategic, legal, and policy changes are suggested to be considered in the nearest future:

To begin with, India needs to vigorously seek a bilateral executive agreement with the United States under the CLOUD Act. Since the overwhelming majority of the data that is used to commit cyber fraud, social media abuse, and phishing attacks are stored on servers controlled by US-based corporations, it is not only a convenient thing to bypass the MLAT process but a necessity in the investigation. This will demand a high-level diplomatic intervention to show conclusively that the data privacy regime of India in the DPDP Act and its revision criminal procedures are rights-compliant and legally valid.

Second, in order to be eligible to such an agreement and be in line with the global human rights, India needs to internally overhaul its investigative procedures to ensure that there is strict judicial control. The formal institutionalization of Section 94 of the Bharatiya Nagarik Suraksha Sanhita, 2023, must be put into practice through guidelines of the Ministry of Home Affairs to make sure that all cross-border digital evidence requests are carried out only by way of judicial summons by a magistrate, and not by police directives. Making the judicial review compulsory and independent, i.e. the magistrate has to explain plausible facts to warrant the data request will meet the US statutory and constitutional privacy obligation as stipulated in the Puttaswamy judgment.

Third, with the UN Convention against Cybercrime to be opened to signatures in 2025. India must use its status as a digital powerhouse to actively influence the adoption of the following protocols of the treaty. India should push hard to have the proposed 24/7 network operationalized to ensure that it works effectively without any subversion of the sovereign right to access data extraction. Moreover, India should be proactive in the process of building strong human rights protection at the Conference of the States Parties, so that the treaty is not used as an instrument of political oppression.

Fourth, following the European Investigation Order example, India needs to become a forerunner of regional, court-to-court direct cooperation mechanisms within the framework of the SAARC or BIMSTEC. Creating direct links between courts in adjacent jurisdictions would reduce the time lag of diplomatic MLAT channels by a factor of four, and would give rise to a localized ecosystem of trust and quick reaction. Lastly, special capacity building on the state level should be directed toward paying significant attention to the legal mechanics of

the international evidence retrieval, training the officers to write the requests that would comply with the foreign probable cause requirements. The prosecution of transnational cybercrime cannot be done by making unilateral claims of extraterritorial jurisdiction. The cyberspace does not respect any sovereign, and the harmonization of domestic criminal codes with the ever-changing global treaties is the most pressing legal issue of the next decade.

Bibliography

i. Bharatiya Nagarik Suraksha Sanhita, 2023, Act No. 46, Acts of Parliament (India).
ii. Bharatiya Nyaya Sanhita, 2023, Act No. 45, Acts of Parliament (India).
iii. Clarifying Lawful Overseas Use of Data Act (CLOUD Act), 18 U.S.C. §§ 2523 (2018).
iv. Constitution of India, INDIA CONST. art. 20, cl. 2.
v. Convention on Cybercrime, Nov. 23, 2001, Council of Europe, ETS No. 185.
vi. Digital Personal Data Protection Act, 2023, Act No. 22, Acts of Parliament (India).
vii. G.A. Res. 79/243, United Nations Convention against Cybercrime (Dec. 24, 2024).
viii. Information Technology Act, 2000, Act No. 21, Acts of Parliament (India).
ix. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation), 2016 O.J. (L 119) 1.
x. *Anvar P.V. v. P.K. Basheer*, AIR 2015 SC 180 (India).
xi. *Arjun Panditrao Khotkar v. Kailash Kishanrao*, (2020) 3 SCC 216 (India).
xii. *K.S. Puttaswamy v. Union of India*, (2017) 10 SCC 1 (India).
xiii. *Om Hemrajani v. State of U.P.*, (2005) 1 SCC 617 (India).
xiv. *State of Maharashtra v. M.H. George*, AIR 1965 SC 722 (India).
xv. Ali, M. A., *Phishing-A Cyber Fraud: The Types, Implications and Governance*, 33 INT'L J. EDUC. REFORM 101 (2024).
xvi. Atrey, I., *Cybercrime and its Legal Implications: Analysing the Challenges and Legal Frameworks Surrounding Cybercrime*, INT'L J. RSCH. & ANALYTICAL REVS. (2023).
xvii. Brenner, S. W. & Schwerha, J. J., *Transnational Evidence Gathering and Local Prosecution of International Cybercrime*, 20 J. MARSHALL J. COMPUTER & INFO. L. 347 (2002).
xviii. Harkin, D. et al., *The Challenges Facing Specialist Police Cyber-Crime Units: An Empirical Analysis*, 19 POLICE PRAC. & RSCH. 519 (2018).
xix. Seger, A., *India and the Budapest Convention: Why Not?*, DIGITAL DEBATES 42 (2016).
xx. Swire, P., Kennedy-Mayo, D., Srinivasan, S. & Srikumar, M., *India-U.S. Data Sharing for Law Enforcement: Blueprint for Reforms*, OBSERVER RSCH. FOUND. (2019).
xxi. Wall, D. S., *Cybercrime and the Culture of Fear: Social Science Fiction(s) and the Production of Knowledge about Cybercrime*, 11 INFO., COMMC'N & SOC'Y 861 (2008).