Hunan Daxue Xuebao/Journal of Hunan University Natural Sciences
ISSN : 1674-2974 | CN 43-1061 / N

DOI: 10.5281/zenodo.21066751
Vol: 63 | Issue: 06 | 2026

THE RISE OF PASSIVE PERSONALITY JURISDICTION IN CYBERSPACE: ASSESSING THE UN CYBERCRIME CONVENTION AND INDIA'S LEGAL RESPONSE

ANANYA DUTT
Assistant Professor, Maharaja Agrasen Institute of Management Studies, Rohini, Delhi.
Email: ananyadutt9@gmail.com

Abstract

The United Nations Cybercrime Convention's introduction of passive personality jurisdiction and its consequences for India's cybercrime framework are critically examined in this essay. It examines how the Convention adds to worries about jurisdictional creep in cyberspace by allowing nations to exercise jurisdiction based on the nationality of cybercrime victims. The paper compares India's current legal system under the 'Information Technology Act of 2000' and the 'Bharatiya Nyaya Sanhita of 2023' with the jurisdictional requirements of the Convention using a doctrinal and comparative legal methodology. In order to improve India's readiness for changing transnational cybercrime threats while preserving constitutional rights, due process, and national sovereignty, the paper analyses important institutional and legal deficiencies and suggests improvements.

Keywords: *UN Cybercrime Convention, Passive Personality Jurisdiction, Cybercrime, Extraterritorial Jurisdiction, Jurisdictional Creep.*

1. INTRODUCTION

Information and communication technologies (ICTs) have been rapidly developing and have transformed the ways in which criminals can conduct their activities, working anonymously and abiding with ease across national boundaries, in ways that were previously unimaginable. Some cybercrimes have become international in nature, such as cyberstalking and attacks on critical infrastructure, and this presents a problem for the traditional principles of criminal jurisdiction, which were originally designed for crimes that had a limited geographic scope. Cybercriminals exploit the nature of digital networks which operate without any border, and states have a great challenge to investigate, prosecute, and prevent cybercrime involving multiple jurisdictions.

The global nature of cybercrime has sparked the creation of new international initiatives that aim to strengthen interstate collaboration and guarantee the creation of a shared legal framework. The Budapest Convention on Cybercrime is still the most important international agreement in this area, although requests for a more widely recognized framework have arisen due to worries about its perceived regional bias and limited global participation. In response, the United Nations adopted the Cybercrime Convention, which seeks to enhance cross-border partnerships, facilitate cross-border investigations and combat new forms of cyber-enabled criminality. The Convention is a significant step towards the control of international cybercrime and is expected to have an impact on national laws and law enforcement practices over the coming years.

One of the most salient features of the Convention is its attitude towards criminal jurisdiction. States have always used territoriality, nationality, and protection interests as the main justifications for exercising criminal jurisdiction. Nonetheless, the Convention now shows a stronger understanding of the possibility of broader jurisdiction, such as that under the passive personality doctrine, which allows a state to have jurisdiction over crimes against its citizens abroad. Although it has only occasionally

DOI: 10.5281/zenodo.21066751
Vol: 63 | Issue: 06 | 2026

been used in international criminal law, the passive personality principle is becoming more and more integrated into the rule of law when it comes to cybercrime.

Significant policy issues are brought up by the growth of passive personality jurisdiction. Critics argue that the broad claim of jurisdiction that is made that a victim's nationality could result in forum shopping, jurisdictional overlap, legal disputes and encroachments on state sovereignty. As a result of such developments, academics have termed the problem as 'jurisdictional creep' the gradual widening of state's criminal jurisdiction beyond its traditional limits in response to emerging security threats. A single action could affect consumers in several countries simultaneously, and the implications of a jurisdictional extension are that much greater in the cyber space.

These developments have a great significance for India. India has the largest digital population in the world, and there has been a significant rise in cybercrime in the past few years. The country's legal framework is already in place and it is primarily governed by the 'Information Technology Act, 2000', and augmented by the 'Bharatiya Nyaya Sanhita, 2023'. But there is not enough research conducted to the role of passive personality jurisdiction in Indian Cybercrime Laws. There are also important questions regarding legal harmonisation, enforcement capacity, due process rights and the maintenance of national sovereignty in the way of how the 'UN Cybercrime Convention's' provisions on jurisdiction interact with India's existing laws.

In spite of the growing attention being focused on international cybercrime law, few studies have examined the implications of the UN Cybercrime Convention's territorial concept of jurisdiction from an Indian perspective. Most of the existing publications focus on the aspects of cybersecurity governance, procedural jurisdiction, and international cooperation mechanisms, while much less attention has been paid to the possible extension of passive personality jurisdiction under the Convention and its impact on national legal systems. This is particularly notable in light of the increasing significance of the victim-based jurisdiction in the realm of cybercrime today.

In light of this, the current paper critically investigates the idea of jurisdictional creep under the UN Cybercrime Convention, focusing especially on the growth of passive personality jurisdiction. It explores the nature and implications of this jurisdiction, the legality behind it and its compatibility with international legal norms and its impact on the cybercrime policy in India. This study contributes to the already ongoing debate on the future of transnational cybercrime governance and on the scope of criminal jurisdiction in the digital age by investigating the interplay between the emergence of international standards and national cybercrime laws.

1.1 Research Problem:

On December 24, 2024, the UN General Assembly unanimously approved an innovative cybercrime pact. Critics, including several companies and human rights groups, condemned it, but several negotiating governments were happy with its adoption. But those who favor and those who oppose the treaty do not yet know just how much more it achieves. The treaty will come into effect shortly when 40 states have ratified it.

A clause in the treaty gives governments the authority to take action against any behaviour that endangers their citizens. This kind of jurisdiction, referred to as passive personality jurisdiction, "has historically been more controversial than jurisdiction based on territory or [the perpetrator's] nationality." In 1989, the French justice minister told the assembly that France's sudden decision to extend unlimited passive personality jurisdiction allow it to try anyone for any crime committed anywhere in the world against any French citizen was "manifest imperialism that is difficult to justify. That way of thinking makes this treaty mean that all states are empires and may make laws in any part

ISSN：1674-2974 | CN 43-1061 / N

DOI: 10.5281/zenodo.21066751
Vol: 63 | Issue: 06 | 2026

of the world, and invade other states' usual prerogative to control and allow the behavior of its citizens.

How might this power be used? Suppose that an American citizen who resides and operates in the USA discovers a database of a U.S. corporation which is set up incorrectly and discloses personal information about Russians, thereby inflicting damage on them. Russia may ask Turkey for assistance in monitoring, detaining, and extraditing the journalist if she travels to Istanbul on vacation, as well as under the cybercrime treaty's passive personality jurisdiction clause. The journalist can attempt to claim that her actions shouldn't be considered unauthorized access by citing the treaty's human rights obligations. The treaty allows for such extraterritorial jurisdiction over foreign conduct of foreign citizens in foreign states even if such rules could be enforced.

Despite not being a signatory to UN Convention, there is some informal convergence with international cyber rules in India's membership of INTERPOL, compliance with some of the Mutual Legal Assistance Treaty (MLAT) protocols and recent discussions regarding access to India's data with international cloud service providers. There are restrictions on this casual interaction, though. Absence of treaty requirements means that Indian law enforcement is not defined by treaty with international law on seeking or exchanging electronic evidence. The present Indian MLAT mechanism has been found to be plagued by various issues such as lack of coordination, unequal agency responses and serious delays in investigations. In addition, the existing gaps in procedural harmonisation between India's existing cyber laws, such as ‘Information Technology Act, 2000’ and international instruments, which are already part of the legal frameworks of the UN or Budapest Convention parties, like uniform frameworks for data preservation orders, emergency access mechanisms and admissibility requirements.

1.2 Research Questions

1) To what degree is the use of the passive personality principle as a foundation for criminal jurisdiction in cyberspace expanded by the UN Cybercrime Convention?
2) How would the addition of passive personality jurisdiction to the UN Cybercrime Convention affect state sovereignty and international law, and would it result in the issue of "jurisdictional creep"?
3) Explore how India's existing cybercrime regime, such as the Information Technology Act, 2000 and the Bharatiya Nyaya Sanhita, 2023, handles issues of extraditing jurisdiction and victim jurisdiction.
4) To what extent is the Indian cybercrime regime equipped to handle the jurisdictional obligations and challenges stemming from the UN Cybercrime Convention and what are the legal reforms needed?

1.3 Research Methodology

In order to examine the jurisdictional framework of the United Nations Cybercrime Convention and its consequences for Indian cybercrime laws, the current study uses a qualitative doctrinal legal research technique. The primary method used in the research is an analysis of sources of law, including international conventions, convention texts, domestic law, court decisions and government reports. The jurisdictional provisions of the ‘Bharatiya Nyaya Sanhita, 2023’, the ‘Information Technology Act, 2000’ and the UN Cybercrime Convention are highlighted.

The study uses a comparative legal methodology in addition to doctrinal analysis to assess how passive personality jurisdiction has evolved in particular jurisdictions and international legal instruments. The

DOI: 10.5281/zenodo.21066751
Vol: 63 | Issue: 06 | 2026

comparative analysis will be helpful to understand the new trends in cybercrime governance and the extent of India's preparedness to implement the Convention's emerging norms of jurisdiction.

The study also uses analytical and critical approaches to examine if the Convention's recognition of passive personality jurisdiction is a legitimate development within the international regulation of cybercrime or a part of a more general trend toward "jurisdictional creep. There is relevant academic literature, government publications, reports from international bodies and academic commentaries that support the analysis and contextualisation of the current debates on cybercrime jurisdiction.

2. IN DEPTH ANALYSIS OF UN CYBERCRIME CONVENTION

The treaty seeks to strengthen preventive measures, promote interstate cooperation, and provide technical support and capacity building for the prevention and combat of cybercrime. Because it acknowledges the shared nature of cyberspace, the treaty focuses particular emphasis on promoting technical aid and capacity-building initiatives to help the impoverished countries. Cooperation, capacity building, prevention, victim care, and child protection are the main areas that the convention aims to address. A critical examination of the convention in light of its overall objectives is crucial.

a) International Cooperation:

The agreement details specific areas where investigations, prosecutions, and legal proceedings will benefit from international cooperation and provides general principles of cooperation. This covers a variety of law enforcement operations, including as gathering and disseminating electronic evidence as well as freezing, seizing, confiscating, and returning the proceeds of crimes. (Mishra, 2024) In addition, the agreement maintains a proper equilibrium between the principle of national sovereignty and cooperation among the nations. The treaty will focus on cooperation and will stipulate that governments transfer personal data as per existing international laws on data protection or national laws. Also, it provides a mechanism to pass an individual's data to a third party if the state that sent the data has given permission to do so. However, in order to be extradited, parties must follow the principle of dual criminality, which means that the act in issue must be recognized as a criminal offense under both parties' domestic laws. States may also refuse to grant extradition if they have a “good cause” to believe that the state is seeking to punish an individual based on their gender, race, language, religion, nationality, ethnic origin, or political opinion. The state may consent to the transfer of criminal proceedings concerning offenses having dual jurisdiction. (Mishra, 2024)

Each party will appoint a central body to receive and carry out requests for mutual legal aid without interfering with current procedures in order to guarantee smooth and timely processing of such requests. A state may refuse reciprocal legal aid if it is an issue of public order, security or sovereignty. (Resolution Adopted by the General Assembly on 27 December 2019, 2020)

The agreement also calls for the establishment of an international round-the-clock network, to facilitate measures such as technical assistance, preservation of stored electronic data, evidence collection and other related measures, and to provide timely assistance during investigations and prosecutions. Further, it fosters the use of the convention as a basis for co-operation among states or bilateral or multilateral agreements. The legislative instrument's jurisdictional guidelines will be followed by the international collaboration that the convention aims to strengthen.

b) Capacity Building:

Cybercrime has become an international problem that is international due to its close connection to the modern world. While some states are still extremely susceptible, others are better prepared to deal with challenges. To bridge this clear gap, particularly in view of the needs and concerns of the developing world, the agreement provides a mechanism for knowledge sharing, ranging from technical

DOI: 10.5281/zenodo.21066751
Vol: 63 | Issue: 06 | 2026

assistance to technology transfer and expertise exchange between the parties. This also involves sharing information to help countries establish relevant legislation and strategies to prevent and tackle cybercrime. Giving states with less funding access to contemporary law enforcement equipment is another aspect of technical help. Capacity can be expanded in other ways besides technical support. There is also a particular focus in the treaty on equipping the human resources of the parties with capacities, including language training, formulation and administration of requests for mutual legal assistance and other relevant tasks. The convention encourages the member governments to make a financial contribution towards the achievement of the objectives to strengthen the work done to support the developing countries. (United Nations Convention against Cybercrime; Strengthening International Cooperation for Combating Certain Crimes Committed by Means of Information and Communications Technology Systems and for the Sharing of Evidence in Electronic Form of Serious Crimes, n.d.)

c) Prevention:

Prevention continues to be the first goal for any person or organization. The convention is based on the importance of collaboration and capacity building efforts focusing on crime prevention and crime response. In order to do this, the convention emphasizes how crucial it is to standardize best practices and policies throughout various jurisdictions. To ensure adequate preventive measures, it also calls attention to the importance of involving a diverse range of stakeholders, such as the public, academia, business and civil society. A crucial aspect of fighting cybercrime is linking and strengthening cooperation among these partners and the law enforcement.

The agreement also promotes the security of the services, goods and client information that service providers provide, and recognises the critical role that service providers play in the prevention process. Additionally, it acknowledges that "legitimate activities of security researchers" are crucial to bolstering overall security. This ensures that security researchers, penetration testers and ethical hackers are not found culpable in future and their efforts are recognized. Intriguingly, the convention is to encourage, facilitate and develop "anti-cybercrime measures and policies" designed to make committing a cybercrime difficult for potential offenders.

This is good, but there is no plan of action for the member states about how they will implement it. It is unclear, nevertheless, if capable authorities will take the seriousness of the offense into account prior to reintegration. States will also need to begin to regularly review their national plans and legislation to respond to the evolving nature of threats.

d) Victim Support:

Article 34 provides measures for the protection and help of crime victims, acknowledging the pressing necessity to do so. It calls on States to act to provide victims with restitution and compensation. The severity of the offence will dictate the actions that can be taken. Examples of this include the need for states to act to ensure that victims of online child sexual abuse, grooming a child for sexual exploitation or victims of the non-consensual broadcast of intimate pictures are physically and psychologically rehabilitated. (United Nations Convention against Cybercrime; Strengthening International Cooperation for Combating Certain Crimes Committed by Means of Information and Communications Technology Systems and for the Sharing of Evidence in Electronic Form of Serious Crimes, n.d.)

e) Child Protection:

The convention prohibits the sale, purchase or possession of anything related to child sexual abuse. Its definition is extended and it also recognises that the production, offering, sale, distribution and possession of such content using ICTs is illegal. Because even serving as a conduit could subject them to criminal liability, the criminalisation of "possessing" and "controlling" such materials could have a

ISSN：1674-2974 | CN 43-1061 / N

DOI: 10.5281/zenodo.21066751
Vol: 63 | Issue: 06 | 2026

substantial impact on service providers and intermediaries. There are written or audio materials in addition to the "visual material" in the article. Similarly, any intentional communication, solicitation, seduction or arrangement for sexual exploitation using ICT is prohibited under the treaty.

2.1 Budapest Convention on Cybercrime and UN Convention:

The cooperation among countries and tools against cybercrime are not new. The most important took place 20 years ago in November 2001, when the Council of Europe adopted the Budapest Convention. The United States, Canada, almost all of Europe, half of South America, and several countries in Africa and Asia were among the 78 parties to the Budapest Convention as of February 202. Seven other countries have signed it and 17 countries have been invited to sign it. The Budapest Convention is about information technology as the medium of committing computer-specific crime. These include the access, modification or interception of electronic data or systems crimes which would not exist without computers. These offences are referred to as cyber dependent crimes or core cybercrimes. A whole range of crimes involve or benefit from the use or misuse of a computer and are often described as 'cyber enabled'. Examples of these include child exploitation and illegal speech. If one thinks about the fact that international criminal treaties generally focus on types of crimes, rather than the way crimes are being committed, the difference between these kinds of crimes becomes apparent. Although motor vehicles are used in the commission of many crimes, there is no international convention to cover the use of motor vehicles in crime (what we can refer to as vehicle-enabled crimes). There are difficulties in targeting the tangible as the target of the crime because this can lead to criminalisation of acts that one state wants to be able to do, such as certain types of speech. If cyber-crimes were to be deemed a criminal act, there would be problems with sovereignty and over-inclusiveness, as international law does not consider the computer to be an illegal object, unlike drugs and counterfeit money.

The Budapest Convention lists nine substantive offences, such as unauthorised access, unauthorised interception, data interference, system interference, misuse of devices, computer-related forgery, computer-related fraud, offences related to child pornography, and copyright-related offences, as criminal offences. This effectively maintains the traditional focus on categories of crimes. These are the initial seven categories of offences that rely on cyberspace. While the latter two are cyber-enabled, the Budapest Convention tightly associates the scope of those two offences with the need for the cyber element. One of such violations is "producing child pornography for distribution through a computer system. Whereas copyright violations and their scope are limited by necessity, the requirements of intent and “commercial scale” and computer indispensability constrain copyright violations.

But the UN cybercrime convention was about whether to continue or discontinue this strategy, between cyber-dependent and cyber-enabled crime. From the beginning the scope of the new treaty posed concerns. States sought to limit the scope of the treaty to cyber-dependent crime, especially those that initially failed to support the committee's founding.

This controversial argument was expressed in the continuous debate regarding the title of the UN treaty. Was cybercrime (also called cyber-dependent crime) or the use of computers for illegal purposes (also called cyber-enabled crime) addressed by the treaty? The General Assembly resolution "to elaborate a comprehensive international convention on countering the use of information and communications technologies for criminal purposes" led to the formation of a committee. It appeared that the convention was intended to be an umbrella document covering the broader category of cyber-enabled crimes, as the wording of the resolution referred to the use of information and communications technologies for criminal purposes and there was no reference in the resolution to a title for the convention. The committee named followed the wording of the General Assembly

ISSN：1674-2974 | CN 43-1061 / N

DOI: 10.5281/zenodo.21066751
Vol: 63 | Issue: 06 | 2026

resolution when the 'UN Office on Drugs and Crime' (UNODC) Secretariat created an agenda for the committee's organisational meeting. But the European Union (EU) delegation disagreed, saying that a "footnote explaining [the title] does not pre-define the title of [the] future conventions.

3. THE EMERGENCE OF PASSIVE PERSONALITY JURISDICTION

Once, an ambiguous or broad treaty was restricted to geographical restrictions. A state's "broad" definition of a crime would not affect the behavior of its citizens in another state, nor would each state have to mold its domestic laws to incorporate a new standard. Indeed, the difference between national states is a feature of international treaties, and most governments and observers will probably view the UN cybercrime convention as following this pattern.

The UN cybercrime convention, however, leads to a blurring of national diversity and, therefore, sovereign rights, by permitting governments to impose their general taxes on foreign activities. The terms of jurisdiction in the treaty, especially those relating to passive personality jurisdiction, which has been the subject of limited scope in the past, indicate an important extension of this limited jurisdiction, which is based on the injury suffered by citizens of a state. The treaty allows each state party to have jurisdiction over crimes committed by any one of its citizens outside its territory. Under certain circumstances, states must recognize and accept claims of "long arm jurisdiction" from other states under the treaty. The states may exercise jurisdiction over cybercrime treaty offences outside their territorial limits through passive personality jurisdiction. Keep in mind the above examples of the deception aspect of Article 13. Now imagine that an American business finds evidence of human rights abuses in its, or a competitor's, overseas supply chain and sends an email press release to a U.S. news outlet, delivers a virtual testimony to a Congressional hearing or texts a law enforcement agent. When an investigation or drop in customer purchases results in a loss to the owners of the foreign company that was subcontracted. Although the American corporation never had any connection or presence in the foreign country, but only in American business, it is still being prosecuted for the falsification of a complaint and attempts to benefit American business. A similar fact pattern can be presented by the firm employee (or any private individual) who made any such electronic communications. The UN cybercrime convention says she could be arrested and extradited on holiday in a third country. The agreement would prevent Washington from objecting to a foreign country's prosecution of Americans for activities outside its territory, even if they believe the United States has a problem with that specific application of the convention, as it would be in the case of international human rights violations.

3.1 Passive Personality Jurisdiction in UN Cybercrime Treaty

Now, the rule is in danger of becoming the exception. The cybercrime convention also introduces compulsory jurisdiction over the territorial and quasi-territorial jurisdiction (including ships and aeroplanes) and discretionary jurisdiction based on the principle of protection, active personality and passive personality. The language in UNTOC and UNCAC which allows for passive personality jurisdiction is precisely the same as in the treaties. Based on record negotiations, it seems that governments did not much think about this short declaration. Early in the process the UNODC Secretariat undertook an assessment of existing legislative instruments and documents regarding combating cybercrime in accordance with the General Assembly resolutions that created the committee. The jurisdiction chapter was negotiated amongst the members of the committee in "informal consultations", private meetings held outside of plenary sessions. Further, in the early stages of the talks, there were several jurisdictional issues raised by member states, often in the context of the need for broad extraterritorial jurisdiction or regarding how to deal with the problem of jurisdiction in cyberspace and the need for "mechanisms for obtaining electronic evidence" that could be located in multiple jurisdictions.

DOI: 10.5281/zenodo.21066751
Vol: 63 | Issue: 06 | 2026

During the first substantive session for instance India had pointed out that “enormous delays” in MLA cases had occurred because the increasingly complex exercise to determine jurisdiction based on the existing classical territorial model had been causing delays.

In addition to the recognition of passive personality jurisdiction, the cybercrime convention is a significant addition to the list of terrorism and violence. Even for crimes well outside the purview of the treaty, it might eliminate most restrictions on the application of passive personality jurisdiction under international law. Individual governments have asserted passive personality jurisdiction and both two recent UN treaties have increased. But, in the context of this case, granting such jurisdiction may give more legitimacy boost than in prior cases; rather than granting it in ad hoc and certain cases, it may secure general acceptance of passive personality jurisdiction.

Despite the number of signatories, the effect of the convention's substantive provisions on this regard was, according to one of the leaders of a digital rights organisation, a "UN treaty is still a huge signalling force. More substantially, infinite passive personality jurisdiction here would further the jurisdictional base in the direction of becoming customary international law, depending on the number of countries that ratify it. Given that the previous UN criminal justice treaties on corruption and transnational organised crime "enjoyed[ed] near universal ratification," the majority of governments will probably sign the UN cybercrime treaty. Moreover, even if a state has no passive personality jurisdiction, ratification of the cybercrime treaty would amount, de facto, to a statement that it is acceptable to do so. This is relevant because one of the elements of custom international law is governments' understanding of what is legal or not.

Additionally, governments may find it challenging to assert that they were backing passive personality jurisdiction in only specific situations (unless they made a reservation in entering the treaty), as they could legitimately argue before to the UN cybercrime convention. In contrast to previous applications of passive personality jurisdiction, its application here is unrestricted by both functional (as in the treaties on organised crime and corruption) and substantive (as in terrorism or violence) limitations.

Indeed, UN cybercrime convention is much more broadly drafted to allow for passive personality jurisdiction than the corruption and organised crime conventions. The transnational organised crime treaty refers to participation in an organised criminal gang, which has numerous restrictive aspects (structure, coordination and intention to commit a major crime in order to obtain a financial or material benefit). For the simple reason that they are individual offences, most crimes are excluded. The corruption treaty is also subject to the same restrictions. Most of the UNCAC crimes are committed by public officials, meaning attempts to bribe citizens of a state would be considered an UNCAC crime. Applicability of passive personality jurisdiction seems to be limited to bribes given abroad of these officials. In this method the formal application of passive personality jurisdiction under the corruption treaty will almost always be less of a formal application of passive personality jurisdiction and more of a formal application of a broad concept of protection to protect the official activity of a government from the harmful effects of official bribery.

States may reasonably claim that they also protested the majority of passive applications of the doctrine of personal jurisdiction following their ratification of both these treaties. A scholar of international criminal law concluded that: "The United States and other common law countries which have enacted such [passive personality jurisdiction] laws have relinquished their objections to passive personality jurisdiction in the context of terrorist crimes, but not other crimes. But that 'unwilling' status of an objector may be overturned, as in the field of the protective principle, by embracing a cybercrime treaty which would allow much wider passive personality jurisdiction. “There,” the practice “is lawful among the signatories to the... treaty,” there could be “very little question.” The UN Convention against Corruption is signed by 191 Parties, and the protective concept is nearly

ISSN : 1674-2974 | CN 43-1061 / N

DOI: 10.5281/zenodo.21066751
Vol: 63 | Issue: 06 | 2026

universally accepted. Moreover, the transition would have a significant impact as the crimes under the UN cybercrime agreement are flexible and open-ended. As mentioned in Section II. This would leave passive personality jurisdiction in the face of cybercrime in an easy and vulnerable position, D infra. Passive personality jurisdiction for a wide spectrum of cybercrimes is only envisioned in the UN convention. Interestingly, Budapest Convention on Cybercrime does not support passive personality jurisdiction in cybercrimes. Neither does the Convention on Combating Information Technology Offences of the Arab League. Those who said that passive personality jurisdiction is suitable for cybercrimes were only for terrorism-related crimes.

4. INDIAN CYBERCRIME AND EXTRATERRITORIAL JURISDICTION

The 'Information Technology Act, 2000' (IT Act), which was passed to encourage electronic governance, regulate e-commerce, and forbid unauthorised access to and misuse of computer systems, is India's main piece of law designed to combat cybercrime. 'Section 66C (identity theft)', 'Section 66D (cheating by personation through computer resources)', 'Section 66E (privacy violation)', 'Section 66F (cyber terrorism)', and 'Section 67 (publishing or transmitting obscene material online)' are just a few of the provisions of the Act that specifically address offences following a significant amendment in 2008. (Information Technology Act 2000, 2000). The 'Indian Penal Code' is still used to prosecute some cyber-related offences, but the 'Bharatiya Nyaya Sanhita (BNS) 2023' has taken its place. The IT Act is the fundamental legal provision for cyber-related offences. 'Sections 318 (cheating)', '351 (criminal intimidation)', and '356 (defamation)' are the equivalent sections of the BNS for cyber-enabled offences. These sections were originally found in the IPC as 'sections 420, 503, and 499', respectively. The BNS still lacks a specific provision that addresses the use of technology in criminal activity, nevertheless. This makes it applicable to both the IT Act and BNS in numerous situations, causing a potential for confusion of jurisdiction, unclear charge wording, and confusion at trial regarding the procedures, and differences in procedures under BNS and IT Act. Operational difficulties for investigators and prosecutors are caused by the absence of a general criminal law framework in relation to specific cyber legislation.

With the creation of the Indian Cyber Crime Coordination Centre (I4C) in 2020 as the national nodal body for cybercrime investigation and capacity building, India's institutional architecture for combating cybercrime saw a dramatic change in recent years. In order to ensure decentralised enforcement, I4C' oversees several arms of operations, such as the 'National Cyber Crime Reporting Portal and the toll-free cybercrime helpline (1930), and promotes the creation of cybercrime police units at the state level. Real-time threat detection, incident response, vulnerability bulletins, international cooperation with other national CERTs, and other tasks are among CERT-IN's duties. It also serves as a regulator by offering industry sector recommendations for cyber security, such as for telecom, banking, and critical infrastructure systems. Log maintenance, breach reporting, and recurring audits are typical instances of these rules. Investigating high-profile international cybercrime offences, especially those involving online fraud networks, cyber extortion, and data breaches, is the responsibility of the Central Bureau of Investigation's (CBI) Cyber Crime Unit. In order to set an example for other areas, some governments, including Maharashtra and Telangana, have established 'Cybercrime Bureaus' with digital forensic labs, technical specialists, and capacity-building programs. However, local infrastructure, coordination, and training advancements are still uneven, and enforcement outcomes differ from jurisdiction to jurisdiction.

The conventional notion of jurisdiction is put to the test by cross-border cybercrime. The main problem is determining location of crime, and also where it ought to be prosecuted, either at the victim's home, perpetrator's home or the source of the resources. The IT Act, 2005, provides for extraterritorial jurisdiction of Indian courts to investigate and prosecute cybercrimes which affect

ISSN：1674-2974 | CN 43-1061 / N

DOI: 10.5281/zenodo.21066751
Vol: 63 | Issue: 06 | 2026

India or Indian nationals acting in Indian corporations. It's referred to as the "effect doctrine. But it's not quite as easy and convenient as it sounds.

Also, there is the "forum non conveniens" doctrine that can also deny or bar jurisdiction where the court's jurisdiction is overlapping with the jurisdiction of other countries or other Courts. One of the most visible examples is multi-jurisdictional hacking events, while in such scenarios, foreign servers harboring harmful information impede Indian investigative agencies from investigating on the basis of sovereignty.

The country's constitutional norms, including sovereignty and political considerations, are also significant hurdles that might be a barrier to implementation and require the assistance of Mutual Legal Assistance Treaties (MLATs). At present, India has signed this agreement with over 40 countries in 2025. The treaties facilitate cooperation between the countries in the collection of evidence and in the exchange of legal documents across countries, which helps in preventing, suppressing, investigating and prosecuting crime.

Such challenges highlight the importance of strengthening international legal cooperation and enforcement, harmonizing cyber law and streamlining processes for tackling jurisdictional challenges in India's cross-border cybercrime prosecutions.

5. THE UNLIKELY PAIR: INDIA AND UN TREATY FOR CYBERCRIME

The current cybercrime regime in India is well-prepared to deal with the jurisdictional requirements provided for in the ‘United Nations Convention against Cybercrime’. Extraterritorial jurisdiction is already represented in the Information Technology Act, 2000 under Section 75 which extends the application of the Act to offences committed outside India in which a computer system, network or computer resource located in India is used. Likewise, the Bharatiya Nyaya Sanhita, 2023 provides for situations where crimes committed outside Indian territories may also be subject to the Indian Criminal Jurisdiction. The provisions accord to India's long history of recognition of the fact that cybercrime often crosses borders and requires flexible jurisdiction.

The UN Convention targets to enhance cooperation, in particular, in the areas of jurisdiction, mutual legal assistance, extradition, information exchange and access to electronic evidence. The Convention also encourages states to have jurisdiction with respect to not only territorial jurisdiction, but also where appropriate, on the basis of nationality and other principles of international law recognised. The present legal position of India thus meets certain basic conditions required for its participation in the Convention.

However, there are issues with the Convention that are not confined to the concept of territorial jurisdiction. A similar issue relates to the increasing recognition of the passively granted criminal jurisdiction, which allows a state to have criminal jurisdiction over offences committed abroad against its nationals. Indian law acknowledges the presence of some type of extraterritorial jurisdiction, but does not explicitly or comprehensively embed a victim-centric approach to the concept of jurisdictional authority for cybercrime offenses. With the increasing prevalence of cyber offences targeting Indian citizens, both domestic and international, this absence of clarity regarding passive personality jurisdiction may lead to uncertainty in relation to investigative jurisdiction, prosecutorial capability and cooperation with foreign jurisdictions.

In addition, the Indian legal regime remains having practical issues with regard to cross-border electronic evidence. Investigations of cybercrime frequently require access to data on servers in a different country or under the control of a multi-national technology firm. The Convention suggests the framework for international cooperation and sharing of evidence, but for India to implement it,

ISSN：1674-2974 | CN 43-1061 / N

DOI: 10.5281/zenodo.21066751
Vol: 63 | Issue: 06 | 2026

the institutions for collecting, preserving and sharing digital evidence should be strengthened. Lack of cooperation due to delays in mutual legal assistance has often obstructed cybercrime investigations and there is a need for more efficient and technologically responsive cooperation mechanisms.

Also of concern is jurisdictional overlap and concurrent claims of authority as discussed in the Convention. Multiple states may have territorial, nationality, and passive personality jurisdiction in one cybercrime incident due to the borderless nature of cyberspace. India's existing law is not conducive to resolving these conflicts. In the absence of such guidelines in the statute, Indian investigators and courts may find themselves in a situation where there are multiple competing jurisdictions involved in a case.

Further, the realisation of the Convention commitments should take account of constitutional provisions concerning personal liberty, due process and privacy. All international cooperation mechanisms that involve cross-border surveillance, disclosure of electronic evidence and access to personal data require to be looked into in light of the Supreme Court of India's recognition of privacy as a fundamental right. Hence, India's ratification of the Convention should be linked to stringent procedural safeguards to meet constitutional requirements and human rights commitments.

Thus, the Indian cybercrime regime creates a good base for compliance with the UN Cybercrime Convention, but is not considered to be “ready” to cover all issues of jurisdiction under the treaty. There are multiple legal changes needed to bolster India's readiness.

In the first place, the legislature should clearly define the scope and limits of the passive jurisdiction in cybercrime cases where the victim is in India or abroad. Second, there is a need for all-encompassing laws on international cooperation in cybercrime investigations which facilitate requests for electronic evidence, mutual legal assistance and extradition. Third, statutory procedures need to be established to deal with conflicts of jurisdiction and to avoid duplicative prosecution caused by overlapping claims of jurisdiction. Fourth, there should be special safeguards in proceedings to ensure consistency with constitutional protections of privacy and due process in cross-border investigations. Last, institutional capacity, such as specialized cybercrime units, digital forensic infrastructure and judicial training programmes, shall be built to help with the effective implementation of the Convention.

To conclude, India has a relatively sophisticated legal structure that provides support for accession to UN Cybercrime Convention. But the growing importance of passive personality jurisdiction and Convention's broad model of international cooperation reveals significant shortcomings in the current system. This means there will have to be targeted legislative and institutional changes to facilitate India's ability to uphold their treaty obligations without compromising constitutional values, legal certainty and national sovereignty.

Convention Requirement	UN Convention Requirement	Existing Indian Legal Framework	Degree of Compliance	Identified Gap	Recommended Reform
Territorial Jurisdiction	Jurisdiction over cybercrimes committed within territory	IT Act, 2000; BNS, 2023	High	Minimal gaps	Continued harmonisation with Convention provisions
Extraterritorial Jurisdiction	Jurisdiction where offences affect interests beyond borders	Section 75, IT Act	High	Cross-border enforcement difficulties	Strengthen cooperation and digital evidence procedures

ISSN : 1674-2974 | CN 43-1061 / N

DOI: 10.5281/zenodo.21066751
Vol: 63 | Issue: 06 | 2026

Nationality-Based Jurisdiction	Jurisdiction over offences by nationals abroad	BNS and criminal procedure provisions	Moderate to High	Fragmented application	Codify cyber-specific nationality jurisdiction provisions
Passive Personality Jurisdiction	Jurisdiction where nationals are victims	No comprehensive statutory recognition	Low	No explicit victim-based jurisdiction	Recognize passive personality jurisdiction legislatively
International Cooperation	Cooperation in investigation and prosecution	MLATs, Letters Rogatory, Interpol	Moderate	Slow procedures	Expedited cybercrime cooperation framework
Electronic Evidence Sharing	Obtaining and preserving electronic evidence	Existing criminal procedure arrangements	Moderate	Delays in foreign-stored data access	Dedicated legislation on cross-border evidence
Extradition	Facilitation of extradition	Extradition Act, 1962	Moderate	Dual criminality concerns	Harmonize cybercrime definitions
Protection of Victims	Victim-centred responses	Scattered provisions	Moderate	Lack of dedicated framework	Victim assistance and compensation mechanisms
Human Rights Safeguards	Protection of rights during investigations	Articles 14, 19, 21 and privacy jurisprudence	Moderate to High	Limited cyber-specific safeguards	Detailed safeguards for surveillance and data requests
Jurisdictional Conflicts	Coordination of competing jurisdictions	No dedicated framework	Low	Forum conflicts	Statutory coordination principles
Institutional Capacity	Develop technical capabilities	I4C, CERT-In, cyber units	Moderate	Resource gaps	Expand training and forensic infrastructure
Data Preservation	Rapid preservation of digital evidence	Partial mechanisms	Moderate	No comprehensive framework	Detailed preservation and admissibility procedures

6. SUGGESTIONS AND RECOMMENDATIONS

1) Passive Personality Jurisdiction and its recognition.

The legislature should explicitly include passive jurisdiction in the cybercrime provisions within India to be able to prosecute crimes committed overseas against Indians.

2) The Comprehensive Cybercrime Cooperation Framework

The government of India should introduce specific laws for cooperation with foreign countries, mutual legal assistance and exchange of electronic evidence collection and analysis in cybercrime matters.

ISSN : 1674-2974 | CN 43-1061 / N

DOI: 10.5281/zenodo.21066751
Vol: 63 | Issue: 06 | 2026

3) Jurisdictional Conflict Resolution Mechanisms

Statutory principles need to be explained to resolve competing jurisdiction claims and avoid tripping over each other in investigations and prosecutions.

4) Improving the Digital Evidence Procedures

International best practices should be followed in the development of uniform standards for the preservation, collection, authentication and admissibility of electronic evidence.

5) Improved Human Rights Protection Measures

The cross border investigative powers must be supervised and have proper procedures in place to meet constitutional requirements to safeguard privacy, due process and personal liberty.

6) Institutional Capacity Building

More resources must be allocated towards the development of digital forensic laboratories, cybercrime investigation units, and specialized training programs for law enforcement, prosecutors and judges.

7) Public Review and Consultation

Domestic cybercrime laws should be reviewed periodically to take account of and remain compatible with the international obligations under the UN Cybercrime Convention.

8) Promotion of International Partnerships

India should build up bilateral and multilateral cooperation mechanisms for quick information sharing, capacity development, and coordinated action in response to transnational cybercrime.

7. CONCLUSION

Cybercrime has become a transnational crime, and the existing principles of traditional jurisdiction are found to be inadequate and need to be complemented with new mechanisms of international cooperation. The ‘United Nations Cybercrime Convention’ is a milestone in cybercrime governance as it provides a universal framework for criminalisation, investigation, exchange and cooperation. The improvement of passive personality jurisdiction, which enables states to assert jurisdiction based on the nationality of cybercrime victims, is one of its most important features. The following study shows the Convention's aim is to enhance states' ability to deal with increasingly complex forms of cybercrime, and also adds to the evolution of criminal jurisdiction outside of traditional state boundaries. This is usually known as "jurisdictional creep" and has led to worries about jurisdictional overlaps, forum shopping, state sovereignty and respect for individual rights in transnational investigations. The analysis also shows that India has a relatively strong legal framework for its participation in the Convention, including in relation to the provisions of the ‘Information Technology Act, 2000’ and the overall framework of the ‘Bharatiya Nyaya Sanhita, 2023’. But there are still wide disparities in the areas of passive personality jurisdiction, the collection of electronic evidence in other countries, competing claims of jurisdiction, and procedural protections for international cooperation. The Indian cybercrime regime is enabled to broadly support the goals of the Convention, but specific legal and institutional changes are needed to facilitate the effective implementation of the Convention. In the end, it is the balancing of effective cybercrime enforcement with the protection of constitutional values, due process, and national sovereignty that will be the challenge for India. The ever-changing landscape of cybercrime demands a nuanced, international and balanced approach to combating it, which India must devise through an appropriate mechanism that does not jeopardize legal clarity and privacy rights

DOI: 10.5281/zenodo.21066751
Vol: 63 | Issue: 06 | 2026

References:

A) Books

1) Gallant, Kenneth S., *International Criminal Jurisdiction: Whose Law Must We Obey?* (Oxford University Press, 2022).

B) Journal Articles

1) Cafritz, Eric and Omer Tene, 'Article 113-7 of the French Penal Code: The Passive Personality Principle' (2003) 41 *Columbia Journal of Transnational Law* 585.

2) Harvard Research in International Law, 'Draft Convention on Jurisdiction with Respect to Crime' (1935) 29 *American Journal of International Law Supplement* 435.

3) McCarthy, John G., 'The Passive Personality Principle and Its Use in Combatting International Terrorism' (1989) 13 *Fordham International Law Journal* 298.

C) Cases

1) *United States v. Klintock* 18 U.S. (5 Wheat.) 144 (1820).

D) International Treaties and Conventions

1) Arab Convention on Combating Information Technology Offences, 2010.

2) Convention against Illicit Traffic in Narcotic Drugs and Psychotropic Substances, 1988.

3) Convention on Cybercrime (Budapest Convention), ETS No. 185, 23 November 2001.

4) Convention on Narcotic Drugs, 1961, as amended by the 1972 Protocol.

5) United Nations Convention against Corruption, 2003.

6) United Nations Convention against Cybercrime; Strengthening International Cooperation for Combating Certain Crimes Committed by Means of Information and Communications Technology Systems and for the Sharing of Evidence in Electronic Form of Serious Crimes, 2024.

7) United Nations Convention against Transnational Organized Crime, 2000.

E) United Nations and International Organisation Documents

1) Ad Hoc Committee, *Fourth Session Consolidated Negotiating Document*, 21 January 2023.

2) Ad Hoc Committee, *Rolling Text of the Draft Provisional Agenda for the Organisational Session*, 17 July 2020.

3) Joint Statement on the Forum for Negotiations and Decision-Making Process Towards the Implementation of United Nations General Assembly Resolution 74/247 on Countering the Use of Information and Communications Technologies for Criminal Purposes, 14 December 2020.

4) Report of the International Law Commission to the General Assembly.

5) United Nations General Assembly Resolution 74/247, 'Countering the Use of Information and Communications Technologies for Criminal Purposes', A/RES/74/247, 27 December 2019.

6) United Nations General Assembly Resolution 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 the Sharing of Evidence in Electronic Form of Serious Crimes*, 24 December 2024.

7) United Nations Office on Drugs and Crime (UNODC), *Overview of Existing Instruments, Recommendations and Other Documents on Countering the Use of Information and Communications Technologies for Criminal Purposes*, UN Doc. A/AC.291/CRP.10, 20 April 2022.

DOI: 10.5281/zenodo.21066751
Vol: 63 | Issue: 06 | 2026

F) Statutes

1) Bharatiya Nyaya Sanhita, 2023.
2) Information Technology Act, 2000.
3) Indian Penal Code, 1860.

G) Government and Institutional Publications

1) Ministry of Electronics and Information Technology, Government of India, 'CERT-In Directions under Section 70B of the Information Technology Act, 2000', 28 April 2022, available at https://www.cert-in.org.in (last visited on 25 June 2025).
2) Ministry of Electronics and Information Technology, Government of India, 'Role and Responsibilities of CERT-In', available at https://www.cert-in.org.in (last visited on 25 June 2025).
3) Ministry of Home Affairs, Government of India, 'Indian Cyber Crime Coordination Centre (I4C)', available at https://cybercrime.gov.in (last visited on 25 June 2025).

H) Newspaper Articles and Online Sources

1) Greig, Jonathan, 'On Eve of Final Negotiations, US Says Consensus Growing Around "Narrow" UN Cybercrime Treaty', *The Record*, 23 January 2024, available at https://therecord.media/consensus-growing-around-cybercrime-treaty (last visited on 25 June 2025).
2) International Chamber of Commerce, 'Global Business Urges Governments to Reject New International Cybercrime Treaty', 13 August 2024, available at https://iccwbo.org/news-publications/news/global-business-urges-governments-to-reject-new-international-cybercrime-treaty (last visited on 25 June 2025).
3) Iyengar, Rishi, Robbie Gramer and Anusha Rathi, 'Russia Is Commandeering the UN Cybercrime Treaty', *Foreign Policy*, 31 August 2023, available at https://foreignpolicy.com/2023/08/31/united-nations-russia-china-cybercrime-treaty(last visited on 25 June 2025).
4) Kerr, Orin, 'Does Obtaining Leaked Data from a Misconfigured Website Violate the CFAA?', *Washington Post*, 8 September 2014, available at https://www.washingtonpost.com/news/volokh-conspiracy/wp/2014/09/08/does-obtaining-leaked-data-from-a-misconfigured-website-violate-the-cfaa (last visited on 25 June 2025).
5) Plumb, Charlie, 'Understanding the UN's New International Treaty to Fight Cybercrime', United Nations University Centre for Policy Research, 30 July 2024, available at https://unu.edu/cpr/blog-post/understanding-uns-new-international-treaty-fight-cybercrime (last visited on 25 June 2025).
6) Rodriguez, Katitza, 'The UN General Assembly and the Fight Against the Cybercrime Treaty', Electronic Frontier Foundation, 26 September 2024, available at https://www.eff.org/deeplinks/2024/08/un-general-assembly-and-fight-against-cybercrime-treaty (last visited on 25 June 2025).
7) 'Global Cybercrime Treaty: A Delicate Balance Between Security and Human Rights', *UN News*, 25 February 2024, available at https://news.un.org/en/interview/2024/02/1146772 (last visited on 25 June 2025).
8) United Nations, 'UN General Assembly Adopts Milestone Cybercrime Treaty', 24 December 2024.
9) United Nations in India, 'UN General Assembly Adopts Landmark Convention on Cybercrime', 24 December 2024.
10) Vibhu Mishra, 'UN General Assembly Adopts Milestone Cybercrime Treaty', *UN News*, 24 December 2024, available at https://news.un.org/en/story/2024/12/1158521 (last visited on 25 June 2025).
11) Council of Europe, 'The Budapest Convention and Its Protocols', available at https://www.coe.int/en/web/cybercrime/the-budapest-convention (last visited on 25 June 2025).
12) Electronic Frontier Foundation, 'Still Flawed and Lacking Safeguards, UN Cybercrime Treaty Goes Before the UN General Assembly, then States for Adoption', 18 December 2024.