CYBER OFFENCES AND DIGITAL JURISDICTION: INTERPRETING "TERRITORIAL JURISDICTION" IN THE DIGITAL AGE UNDER BHARTIYA NYAYA SANHITA

Aritra Saha, BBA LLB, SOA National Institute of Law, Bhubaneswar, Odisha

ABSTRACT

The cyber world has brought the world as a global village in communication and trade but has also presented a major problem to legal systems in dealing with cyber crimes. The traditional jurisdictional principles that focus on a geographical area have difficulty dealing with borderless and anonymous cybercrime. It is against these developing cyber realities that the critical paper is based on the concept of the territorial jurisdiction according to the Bhartiya Nyaya Sanhita (BNS). It explains the drawbacks of the classical principles of jurisdiction in penalizing digital crimes and what BNS can accomplish to revise and reformulate the law to deal with cybercrimes that afflict India. The research situates Indian legal provisions such as the Information Technology act and the procedural laws with a focus on the principle of extraterritorial jurisdiction which has been bestowed on the cyber offences whereby the harm has been committed in the Indian territory. It goes on to contrast the international law tools like the Budapest Convention and the new United Nations one on Cybercrime to show the global ways of cooperating to address jurisdictional issues. Indian and other jurisdictional landmark judicial cases are examined to find the ways in which courts approach the issue of territorial jurisdiction in cyberspace, and the significance of the effects doctrine and protective principles. Understanding the obstacles to synchronization of jurisdictions, cold cyber space, and anonymity of technologies, this paper gives an appropriate proposal of improvements to law with a set of recommendations: jurisdictional regulation in BNS, increased global collaboration, greater mutual legal assistance agreements, and extra capacity building in policing.

Keywords: Cyber offences; digital jurisdiction; territorial jurisdiction; Bhartiya Nyaya Sanhita; cybercrime; international law; cross-border enforcement.

Introduction

The conventional understanding of territorial jurisdiction based on a physical formation of states has always remained the bedrock concept of identifying the power of the legal system to administer laws and resolve conflicts. It is based on sovereignty and the Westphalian system and views jurisdiction as territorially bounded by their boundary of nations. This premise has however been thrown radically out when the cyberspace was born and the internet based on its explosive growth threw radically challenged this premise. The offences always cross the geographical boundaries thus perpetrators can commit a crime in a jurisdiction, harm it in another and they complicate the establishment of the location of the crime and the law that should apply. This cyberspace borderlessness and the anonymity of internet actors have revealed the weaknesses of the normal jurisdiction and has generated law gaps and conflicts. There has been a resultant concern on how to comprehend the concept of territorial jurisdiction in the digital age, which has proved to be a major legal issue that is of international concern.[1]

The Bhartiya Nyaya Sanhita (BNS) in India seeks to reform and streamline the legal provisions in India to incorporate even the cyber offences and jurisdiction provisions. The BNS should negotiate the constitutional and statutory values of India and reality of the digital technology and global connectivity. This will require a subtle concept in dealing with the territorial jurisdiction- a concept that extends beyond the geographical features of the land to include the impacts of activities within the Indian territory, the location of the victims, as well as the goal of the digital behavior. With the analysis of the Indian laws, including the Information Technology Act, general international treaties, and some of the key case laws, the paper discusses the shifting judicial interpretations and changes in the doctrine. Finally, the paper aims to establish what can be done in terms of practical solutions on how to improve the legal framework in India under BNS to enable the jurisdictional nuances associated with the process of dealing with cybercrimes.

Cyber Offences Defined and In Scope

Cyber crimes, also known as cyber offences are criminal activities that are aimed at, or that

[1] Navigating Jurisdictional Complexities in the Digital Age, THE LAW INSTITUTE, https://thelaw.institute/regulation-of- cyberspace/navigating-jurisdictional-complexities-digital-age/ (last visited Nov. 4, 2025)

touch the computers, communication systems and digital information. These kinds of offences take advantage of the special attributes of the digital target, including simplicity of information copying, anonymity, and global connectivity, to inflict damage, theft of money, invasion of privacy or critique of fundamental systems.[2] Cybercrime has developed significantly out of the mere hacking to multivariate cybercrime such as ransomware attacks, phishing, identity theft, digital sexual harassment, cyber terrorism and misinformation campaigns.

Correspondently, Indian legal definitions have changed. The first step was made by the Information Technology Act, 2000 that defined punishable cyber acts and gave legal concept to electronic contract, digital signature and stipulated the fundamental cybercrime penalties. Nevertheless, with the rapid development of technology, nowadays it can be seen that the Bharatiya Nyaya Sanhita, 2023 has already included cyber offences as a part of the main penal laws in lieu of penal colonial-era laws, and this indicates a more wide-ranging and more modern understanding that fully encompasses the cybercrime within the criminal statute of India, in terms of its seriousness and comprehensive impacts on persons, property and the State.[3]

Categorization of Cyber Offences

The Indian law groups the cyber offences according to the type of victim and the damage used:

Criminal Acts against the Person

The category includes those crimes that breach personal security, privacy and dignity:

- Hacking and Unauthorized Access: This refers to the activity of gaining access or modifying computer resources without authorization usually with a view of stealing data, shutting down systems, or manipulating information.

- Data Theft and Privacy Violation: Unlawful access to personal, financial or sensitive

[2] Adv. Darpan Magon, Cyber Crime Punishments under BNS (Bharatiya Nyaya Sanhita), MYJUDIX (Feb. 17, 2024, updated Feb. 20, 2024), https://www.myjudix.com/post/cybercrime-punishments-under-bns-bharatiya-nyaya-sanhita

[3] Bandu B. Meshram & Manish Kumar Singh, Bridging Physical & Cyber Crimes in Bharatiya Nyaya Sanhita 2023, 11 J.

information which is electronically stored.

- Cyberstalking/Harassment: Repetitive and unwanted internet communication or surveillance which produces harm or apprehension.

- Identity Theft and Fraud: This involves committing or deceiving using the identity or the credentials of another.

- Cyberbullying and Defamation: Message threatening, harmful, or fake dissemination, derogating the reputations of the victims within a digital system.

Such crimes usually cause psychological and emotional damage and intrusion of privacy.

Offences Against Property

Cyber crimes that affect or concern property rights which are in most cases economic and intellectual property rights:

- Phishing and Social Engineering: Fraudulent methods of making the victims provide confidential information.

- Ransomware and Malware: This is malicious software that is used to encrypt or corrupt files and their restoration requires payment as ransom.

- Financial Frauds and Scams: Innovative online frauds that rob an individual, business or financial institution.

- Piracy and Copyright Violations: Starting with unauthorized reproduction and distribution of digital materials that is subject to the rights of creativity and economy.

- Cyber Money Laundering: Hiding illegal riches using digital currency.

Such offenses cause loss of huge amounts of money, which draws doubt on the digital infrastructures.

Offences Against the State

More serious as they jeopardize the sovereignty and the security of the people:

- Cyber Terrorism: Attack with the use of cyber tools through the interference with a critical infrastructure, communications or government operations.
- Cyber Espionage: The illegal gaining of classified company or government information, to gain political or economic benefit.
- Online Sedition and Hate Speech: Publication of the content aimed to provoke violence or division of peace.
- Hack on Government Websites or services: Hacks that seek to destabilize government systems or are used to manipulate democratic processes.

Information Technology Act, 2000: Introduction and Characteristics

India has its most significant legislation that deals with electronic governance, e-commerce, and cybercrime called the IT Act, which was passed in 2000 and improved significantly in 2008 and subsequent years. Its objectives include:

- ➢ Sanctioning electronic records and electronic signatures to support safe e-transactions.
- ➢ Establishing digital contractual and delayed payment legal frameworks.
- ➢ Stating and punishing a wide range of cyber crimes.
- ➢ Truly empowering police and legal systems to respond with a hand of law to cyber crime.
- ➢ Monitoring the roles of the intermediaries on online platforms.
- ➢ Stepping up a system of asking redressing grievances and adjudication.

The main characteristics of the IT Act are:

- ➢ Extra-Territorial Jurisdiction: The Act extends to the activities outside India that have an impact on the Indian systems or the person and an international cyber criminal who influences India is prosecutable under the Act.

- ➢ Electronic Records and Signatures: Section 4 and 5 are used to guarantee that the electronic records and signatures are legally enforceable.

- ➢ Certifying Authorities: Framework The issuance and regulation of the digital certificates authenticating digital signatures.

- ➢ Cyber Appellate Tribunal: Special adjudicatory body on the disputes on the IT Act, which is however being streamlined by recent reforms.

- ➢ Intermediate Liability and Safe Harbors: In Section 79, the intermediaries receive conditional exemption of the third-party content so long as due diligence is done.

- ➢ Government Power of Interception and Blocking: The provisions in sections 69 and 69A authorize the state to intercept, monitor or block internet messages and content, which have impact on the sovereignty, civil order or security.

The Information Technology Act contains some Penal Provisions

The IT Act contains broad penal provisions against the diverse kinds of cyber offending:

- **Section 43**: Provides penalties and loss of money as a result of illegal access, data theft, woman of virus, service denial, data corruption and identity theft.

- **Section 66**: Imposes jail time (to three years), or fines on hacking and other crimes of a wrongful loss.

- **Section 66B to 66F**: These include computer resources stolen or identities being stolen, cheating through personation, privacy invasion, and cyber terror and the punishment provided to offenders is based on the extent of violating the law with penalties going as high as life imprisonment.

- **Sections 67 to 67B**: the publication or other transmission of obscene data, child porn or sexual information, imprisonment penalties to seven years, and considerable fines.

- In **Section 72**: Confidentiality in information is secured and any disclosure is

penalized.

- **Section 74**: Imposes the punishment in case of the neglect of protecting electronic signatures or encryption keys.

Such penalties formulate a deterrent effect, and accordingly, punish the cybercrime offender based on the consequences and the harm to society.[4]

Bharatiya Nyaya Sanhita, 2023: The Transformative Legal Framework

The new criminal code will be the BNS, which will be used in place of the IPC as the main criminal code starting in mid-2024. The cyber offences in the BNS will be integrated into the substantive legal framework more thoroughly and clearly:

➢ Organized Cybercrime (**Section 111**): This section applies to cyber criminal activities by syndicates and therefore imposes severe effects such as death penalty on offenders whereby a fatality or grievous injury is caused by cybercrime.

➢ Digital Theft and Fraud (**Sections 316** and **318**): Railroads stealing and defrauding using digital

means are highly dangerous penal offences and correspond to stealing tangible property.

➢ Cyber Harassment, Cyberstalking, Sexual Harassment Provisions: codify cyberspace harassment and stalking with particular penalties to bring more attention to cyber violence.

➢ Cyberterrorism: Have been expanded to include digital sabotage of critical infrastructure, digital disinformation which creates panic and social unrest.

➢ Intermediary Accountability: Force the digital platforms to act in accordance with the legal government requirements to heed the lawful government orders, moderate

[4] INDIAN INSTITUTE OF BANKING & FIN., CYBER LAWS IN INDIA, in IT SECURITY (Taxmann Publishers), https://www.iibf.org.in/documents/cyber-laws-chapter-in-legal-aspects-book.pdf

the content, and cooperate in government inquiries.

The fact that the BNS addresses cyber offences as a core criminal issue illustrates the liberal nature of Indian jurisprudence about the issues of cyberspace and the need to consider cyber offences a part of core criminal issues.

Distinctions between Cybercrimes and Traditional Crimes

Cyber criminality varies in some basics:

- Location and Jurisdiction: Offenses occur in cyber space where no physical boundaries exist to be used as grounds of territorial jurisdiction.
- Anonymity: Offenders use anonymizing tools and make the attribution hard.
- Evidence Nature: Evidence consists of something intangible, it is digital and must be handled and verified by special technical means.
- Fast Pace of Change: Cyber threats change dynamically, and legislative and enforcement changes are to be frequent.
- Multiplicity of Offender Roles: Multiplicity- The same person or group of people tend to collect several roles- the creator, the distributor and the user.
- lobal Effect: Any cybercrimes can spread rampantly across borders in real time as opposed to the localized traditional crimes.

Laws such as the IT Act and BNS are meant to counter these demands by availing more flexible and strict legal measures and mechanisms to deal with the complex demands of cyber offences in India.

Traditions in the definition of Territorial Jurisdiction in Criminal Law

Under the Code of Criminal Procedure, 1973 (Sections 177-186) conceived essentially

In India, the territorial jurisdiction concept on criminal law is largely enshrined in the Code of Criminal Procedure, 1973 (CrPC) particularly in Sections 177 to 186. Chapter thirteen of

the CrPC talks a lot about the jurisdiction of criminal courts in enquiries and trials.[5]

The basis principle set forth in section 177 of the CrPC is that each and every offence should, as a rule, be investigated and prosecuted by a court in the jurisdiction area of which the offence had been perpetrated. Section 2(j) of the CrPC defines the local jurisdiction as the geographical area under which a court or magistrate can exercise his powers. The basic justification is functional--ideally justice is to be served in places close to the crime that took place so that evidence and witnesses are close-by and society has control. Sovereignty of states and administrative convenience also are considered in this territorial demarcation.[6]

Section 178 extends this to oblige courts to ask or prosecute offences, which occurred partly in one territory and partly in another or in different areas of localities. Therefore, an offense which is continuous or happens across more than one locality can be prosecuted in one such jurisdiction where any element of the offense has occurred.

Section 179 states that, an offence can be tried at any court whose jurisdiction one of the events occurred or consequences been caused by the act of commission. This is in recognition of the fact that the location of the harm is also important as is the location of the criminal action intending.

Moreover, S.180 through S.182 address exceptional situations, including where an offence is concurring with other offences (e.g. conspiracy) or whereby an accused circumstance is apprehended outside of the primary location. The CrPC also acknowledges the fact that some offences such as dacoity, abduction and robbery can be conducted in any court within the district of the occurrence of the accused or the recovery of the stolen property.

In this way, the principle of the primacy of territoriality or proximity between the place of crime and the court, which the jurisdiction is anchored on, is established in the CrPC, having given clarity on where a criminal may be tried and given the physical site of the criminal activity centrality.

[5] Wikipedia, Code of Criminal Procedure, 1973 (India), https://en.wikipedia.org/wiki/Code_of_Criminal_Procedure_(India)
[6] Drishti Judiciary, Jurisdiction of Criminal Courts, DRISHTI JUDICIARY, https://www.drishtijudiciary.com/to-the- point/bharatiya-nagarik-suraksha-sanhita-&-code-of-criminal-procedure/jurisdiction-of-criminal-courts

The Law of the Law of the Place Where the Offence is Committed (i.e. the Lex Loci Delicti Commissi)

One of the basic international legal principles of criminal jurisdiction is referred to as lex loci delicti commissi, which literally translates to the law of place where the crime was committed. Using this rule, jurisdiction and law would be identified by determining the place of the wrongful act. This principle is well caught in the history of domestic and international law, offering predictability and adhering to the sovereignty of countries.

Take an instance whereby a theft takes place in the state of Delhi only the courts under the jurisdiction of Delhi can prosecute the accused in that crime but not under an exception like the accused being caught in a different state. The territorial presupposition acts as a control measure so that the local laws are applicable, and the enforcement bodies are practically under control of the investigation and prosecution.

Other jurisdictional principles supplement the lex loci delicti principle: nationality (jurisdiction founded on the nationality of the offender) and universality (as an heinous offense such as piracy or genocide) but territorial jurisdiction is the paradigm of an ordinary crime.

The Principles of territorial, Nationality and Universality

In addition to lex loci delicti, jurisdiction to commit crime may rest on:

- Territorial Principle: jurisdiction of wholly or partly committed acts on the territory of one of the state.

- Principle of nationality: Principles Jurisdiction in accordance with the nationality of the criminal offender or the nationality of the victim no matter where the crime occurs. India claims this, e.g. in its prosecution of Indian citizens who have committed crimes in other countries.

- Passive Personality Principle: The principle of jurisdiction on the victim of the nationality.

- Protective Principle: The right to prosecute actions which pose a threat to the security

or sovereignty of the state even when carried out in another country.

- Principle of universality: The jurisdiction over the crimes that are universally condemned (e.g. piracy) regardless of the place of their occurrence.

The principles of extraterritorial jurisdiction are contained in the Section 3 and 4 of the Penal Code of India, which permits the trial of acts committed outside India but the consequences of these acts are experienced in India or the accused is in India.[7]

Why the Conventional Jurisdiction does not work in Cyberspace

Territorial model is extremely restricted to use in the case of cyber offences due to nature of the internet and digital technology which is borderless:

1) Multiplicity of jurisdiction on a Single Offence: Cybercrimes tend to have actions that are launched in one jurisdiction, handled by servers in another, and afflict victims located in different places in the world. A single geographical location becomes hard to identify thus posing confusion on the criminal law enforced by a particular state.

2) Anonymity and Remote behavior: The perpetrators have the capability of hiding their identities anywhere on earth, and their actions cannot be legally enforced as it may be impossible to track them down.

3) Delayed or Distributed Harm: Certain computer crimes produce harm either over time, or by accessing more than one location, and the logical locus of crime is difficult to establish.

4) Intermediary Roles and Multi-Stakeholders: The Internet service provider, cloud service and digital platform can be based in various countries or jurisdictions, and thus enactment becomes more complicated.

5) Dissimilar Legal Standards and Procedures: The difference in international cyber laws and privacy regimes provokes conflicts in the assertive jurisdiction and mutual

[7] Criminal Law, LLOYD LAW COLLEGE, https://www.lloydlawcollege.edu.in/blog/criminal-law.html

legal assistance.

In the digital era of technology, Territorial Jurisdiction

The Idea of Cyber Territoriality

The concept of territorial jurisdiction has traditionally been associated with the ability of a state to control behavior and to implement laws to the territory within a specific geographic boundary. But cyberspace, or a non-location developed with the help of digital networks, does not respond to these geographical regulations, and it is necessary to develop the concept known as cyber territoriality. The concept of cyber territoriality tries to enforce the jurisdictional values on a fundamentally borderless online space that is a space involving virtual transactions and interactions between various physical and legal jurisdictions all at the same time.

In ancient territoriality, the jurisdiction is obtained based on sovereignty over the land and the resources within defined boundaries. Cyber territoriality, on the other hand, is oppositional and subjected to fragmentation on the reason of non-physicality of cyberspace. Although the digital networks, which the physical server, cables, and physical infrastructure manage have their geographic node, the working nature of the internet supersedes these location points with the virtual links and encrypted communication providing real-time access all over the world. Therefore, the jurisdictional issue of determining jurisdiction over activities that are performed in or involving cyberspace poses challenges to states forcing them to innovate and adapt laws.

How the Internet crosses National Borders

Inherent in the architecture of the internet, the territorial jurisdiction is subverted by pushing the flow of data through very many interconnected, international networks. One cyber crime has an ability to cut across more than a number of jurisdictions within just a few seconds making it unclear where the criminal activity originated. As an example, the hacker in one nation can use the server infrastructure in another country to breach the information of victims in several other jurisdictions.

Such a vagueness in demarcation causes the issue of place of act vs. place of effect in cybercrimes. Place of act and place of effect: The place of act means where the offender

commences the cyber act (e.g. where someone begins to be hacked into) and the place of the result where the damage is caused or the victim is harmed. This dichotomy, in contrast to both conventional types of physical crimes that are confined to a

location, provides the complexity of jurisdiction: is it the place of the origin of the act or the location of its impact that needs legal action? This makes these places commonly very different as the cyberspace is diffused and instantaneous, and a variety of states are competing to have jurisdiction.

Such duality compounds traditional legal principles and makes it imperative to develop flexible and inclusive jurisdictional models that can provide room to distributed reality of cyberspace world.

Jurisdiction theories of Cyberspace

To combat the given challenges, the international law and national jurisdictions impose a number of critical principles or theories of jurisdiction to the offences of cyberspace. They are Objective Territoriality Principle, the Effects Doctrine, the Protective Principle, and Universal Jurisdiction. Both of them offer a premise under which jurisdiction can be extended or curtailed in the digital space.

Objective Territoriality Principle

The objective territoriality principle extends the jurisdiction onto any of the states on the territory of which any constituent act of a multi-state crime is initiated, irrespective of the location of the harm. The jurisdiction is applied to cyberspace whereby a country can exercise authority over cyberspace activities initiated inside its borders although the harm to other countries occurs. As an example, when a cybercriminal transmits fraudulent emails using such servers in Country A and defraud victims in Country B, Country A can claim jurisdiction since that country is the beginning of the criminal act.

This principle tries to base jurisdiction on factual point of origin of the cyber crime to solidify the relationship between the sovereign capacity of states and actions that are physically emanated by it.

Effects Doctrine

Effects doctrine can justify jurisdiction on the grounds of causing harm or injury due to the commission of crimes without paying attention to the intended location of the perpetrator. A country that loses its nationals or infrastructure to an attack launched from an external location can assert jurisdiction to the offenders in cybercrime. The doctrine prefigures the safeguarding of interests of a state since it dwells upon phenomena that are experienced within its border.

Such a strategy finds a great number of adherents in the context of international cyber jurisprudence since this way of reaction will enable states as victims to take action even when criminals are out of their respective physical domains. In a case in point, when the malware that is hosted in Country X goes to shut down financial institutions in Country Y, the Country Y has the option of prosecuting the criminals via the effect-based jurisdiction model.

Protective Principle

The protecting principle authorizes a state to have jurisdiction over foreign action which poses threat to its security, sovereignty or government in any other territory. This has been particularly applied with cyber terrorism, espionage, or offenses that pose threat to the national critical infrastructure that the state regards as having almost exclusive rights to protect vital operations.

This implies that in cyber law states prosecute and offer prosecution to those who engage in cyber crimes (in foreign countries) that threaten the security or sovereignty of the state, irrespective of the nationality or location of the offender. To a large extent, the principle supports the extraterritorial laws regulating cybercrimes in relation to threats against national order and security.

Universal Jurisdiction

Universal jurisdiction applies to some of the most vile offences that are universally understood to be criminal without regard to the place of jurisdiction of a national state like torture or piracy or murder. Although less prevalent within cyber law, there has also been discourse of cyberterrorism or computer crimes against the digital common heritage of humanity (such

as attempts to take down world web infrastructure) that should fall under the reach of universal jurisdiction prosecutors.

Be it controversial and rarely utilized, universal jurisdiction is an ideal concept of law responding to the transnational issues, which different states are not left to handle unilaterally.

Law-Extraterritoriality Judicial and Academic Controversies

The trans-national nature of cybercrime has triggered a tremendous judicial and scholarly debate of the validity, boundaries, and scope of extraterritorial jurisdiction in cyberspace.

Courts all over the world have inconsistently applied effects doctrine and protective principle to cyber cases judicially. Cases that were landmark like the case of United States v. To prosecute foreign hackers over harm inside the US, Ivanov authenticates the application of effects doctrine by the US. In the Information Technology Act, 2000 also, Indian courts have applied a flexible interpretation of territorial jurisdiction and have broadened the doctrines of effects and protective jurisdiction especially in the area of cyber terrorism and internet frauds against Indian citizens.

However, there are difficulties of juggling jurisprudential sovereignty and enforcement in a real world where courts are faced with diplomatic sensitiveness and a possible conflict of claims. The courts promote courtly goodwill and moderation and assert the need of judicatory assertion to guard against cyber damages to the citizens and interests.

In the academic world, the sufficiency of traditional territorial sovereignty in the cyberspace has been debated, with many suggesting that legal pluralism is necessary or some form of functional jurisdiction along the lines of activity centers (i.e., origination, reception, damage). Others are in support of international harmonization by way of treaties and cyber norms so as to avoid conflicting jurisdiction and instead fostering co-operation. Others criticize a danger of overreach that may result in conflict, violation of privacy and online rights.

The controversies focus on the adaptations of the meaning of jurisdiction between state sovereignty and the fluid nature of cyberspace on the balance between enforcement, fairness, and cross-border cooperation.

Cyber Jurisdiction and Bhartiya Nyaya Sanhita (BNS)

Summary of Provisions of Jurisdiction under the BNS

The Bhartiya Nyaya Sanhita (BNS), to be introduced on July 1, 2024, supersedes the Indian Penal Code (IPC), with the target of modernizing the criminal law (becoming a powerful, simplified and unified criminal law) and enhanced to address the modern times such as cybercrime. Its provisions of the jurisdiction are related to the IPC, Section 3 and Section 4- but with important modifications for the digital era.

IPC section 4 (since amended and enlarged in BNS) gave extraterritorial jurisdiction in cases where the offenders were Indian citizens, or the offence committed outside the territory of India resulted in injury in the territory of India. The BNS goes on to accept and broaden this territorial claim on cyberspace by arguing that it has jurisdiction not only over Indian soil but also on Internet offences to Indian interests, which substantiates closely with the international concept of jurisdiction in the cyberspace.

Others that are critical to the cyber jurisdiction in BNS include those that acknowledge:

- **Section 111** (Organized Crime including Cyber Offences): This incorporates the cyber criminal organizations like big hacking companies or cyber fraud syndicates. The strict punishment may be considered in this section and includes life imprisonment or death penalty where cyber-crimes occur leading to death or serious injuries.

- **Section 316** (Theft in Digital Form): Coercively makes it a crime to steal digital property (data, money or intellectual property) since it is acknowledged as the same in the law as any other kind of property.

- **Section 318** (Digital Cheating and Fraud): Addresses misrepresentation, phishing and online scams and offers definite digital liability on crimes.

- Privacy breach, cyberstalking, harassment, cyber terrorism and misuse of digital evidence provisions are indications of a modern perception of criminal harm in technology-based crime.

In such a manner, the BNS could no longer be confined within the territorial limits of the IPC but is now operated in a wider, effect-focused and participation-conscious jurisdictional system that makes it possible to prosecute cyber offences regardless of the geographical location of the offender.

The Major Changes or Innovations over the IPC

The BNS has some significant improvements over the IPC in contracting cyber jurisdiction:

- **Clear Inclusion of Cyber Crime in the Primary Criminal Code**: The IPC has put cybercrime in the shade in most parts of the crimes under the IT Act and the general IPC, which BNS reflects by putting cyber offences in the mainstream under substantive sections, which also highlights the fact that digital crimes are neither inferior in level to ordinary crimes.

- **Broadened Territorial jurisdiction**: BNS facilitates a more expansive territorial jurisdiction in that crimes originating in India can be prosecuted under the doctrine of effects in that the crime would be subject to its jurisdiction in spite of the physical location of the offender-people have seen BNS address the traditional gaps in prosecuting cross-border cyber crimes.

- **Organized Crime Incorporation**: Cybercrime is identified as an organized crime in which the penalties are harsher and also allows special investigation processes applicable to the syndicate and networked criminality that are common in the cyberspace.

- **Emphasis on Digital Evidence**: BNS trains well with the Bharatiya Sakshya Adhiniyam (BSA) that focuses on admissibility and integrity of electronic evidence, which is necessary in successful cybercrime prosecution.

- **Legal Clarity and Definitions:** The BNS has offered clearer legal definition of computer crimes and other related terms, which lacked transparency under the IPC and IT Act.

- **Higher Sensitivity to Privacy and Digital Rights:** BNS Post-Puttaswamy

decisions, BNS takes into consideration more subtle ways to protect privacy at the expense of a state interest in regulating cybercrimes.

- **National Security and Cyberterrorism**: Clarifying cyberterrorism: Concrete legal measure of cyberterrorism with harsh repercussions indicates the Indian concern in protecting the cyberspace as a vital infrastructure.

BNS Legislative Intent in the Cyber Challenges

A legislative purpose of BNS is an active, futuristic mode of understanding that:

- It was the fast development of technology which was causing the emergence of new and sophisticated forms of crime that are not based on the traditional territorial and evidentiary paradigms.

- The need to reform the criminal laws not only in their content but also in the area of the jurisdiction,

  standards of the procedures and rigour of the evidence.

- The need to have better capability to deal with the organized, large-scale cybercrime using cross- jurisdictions networks.

- Safeguarding of personal rights such as privacy, freedom of expression, and safeguarding against unreasonable action of the state against an offender verses against strong the control over cybercrime.

The BNS is the answer of India to the complex environment of cyber cyber threats and is designed to empower law enforcers, courts and accept the courage of league prosecutors by developing a common code, adapted to the digital world.

Correlation between BNS and the Information Technology Act, 2000

The BNS is not intended to replace, but to complement, the scope of the Information Technology Act, 2000 (IT Act) and its subsequent amendments in coming up with the current cyber regulatory system in India:

- IT Act as a Cyber-Specific Statute: Addresses-technically, such as digital signatures, electronic governance and it provides specific offences like hacking, data theft, and intermediate liability.

- BNS as Core Penal Framework: You have core criminal law of substantive law, which deals with stealing, cheating, and assaulting, as well as organized crime, including cyber-forms of these types of crimes.

It is possible to see the synergy here with procedural and technical rules in the IT Act (e.g., digital evidence gathering, certification authorities) facilitating the use of substantive law rules by BNS. These laws combined facilitate a more systematic, stratified method to the law where technological parameters are administered by the IT Act and the penal sword by the BNS.

Is BNS Adequate in Sealing Jurisdictional Leakages in the Cyber Offences?

The BNS especially moves in a similar direction as compared to the IPC because it takes on a broader and more holistic geographic jurisdiction concept that is more appropriate in cyberspace- the effects doctrine, the nationality concept and the concentration on organized crime components. It further reflects on extraterritorial jurisdiction whenever Indian interests are subjected to find a gap in the classics so that cybercriminals can evade prosecution as a result of lack of jurisdiction.

Yet, there are still problems of implementation:

- Blistering Social Change: New cybercrimes such as AI-based deepfakes or massive assaults using botnets necessitate a constant overhaul of law despite original BNS writings.

- International Cooperation: Legal foundation in jurisdiction through BNS offers, but needs to be brought to the ground through treaties, MLATs and diplomatic alignments in development.

- Capacity Gaps: Police and courts should have the capacity to manage technical complexities of cyber jurisdiction problems constantly.

Although the BNS is an important development towards the holistic jurisdiction in cyber criminals, continuous policy, procedure, and bilateral endeavor is a necessity to convert the statutes to effective deterrence and justice delivery on cyberspace.

Cyber Jurisdiction International Framework

Budapest Convention on Cybercrime (2001)

The first and the most important international convention against crimes including those carried out through the internet and computer networks is the Budapest Convention which was adopted by the council of Europe in 2001. It aims at balancing domestic law pertaining to offense dealing with cybercrime, develop improved investigative procedures as well as increase cooperation among nations in the successful prosecution of cybercrime.

The Convention outlines:

- Substantive Criminalization: It provides and otherwise criminalizes central cyber crimes, such as unlawful access (hacking), unlawful interception, data disorder, system interference, device misuse, computer-related forgery, computer-related fraud, child pornography related crime and copyright infringement through electronic means.

- Procedural Powers: It permits the use of national laws which give powers to the authorities to provide the procedures like faster preservation of the stored data, production orders, search and seizure of the computer data, real-time gathering of the traffic data, and interception of content data.

- International Cooperation: One of the greatest innovations is that it has a system of international cooperation, such as extradition, mutual legal assistance (MLA), spontaneous exchange of information, the creation of 24/7 points of contact, and the process of assisting the investigation across borders promptly and efficiently.

- Protections: The Convention acknowledges basic rights and therefore emphasizes proportionality and deference of human rights in accordance with the international guidelines such as the European Convention on Human Rights and International covenant on civil and political rights.

Over 80 states are either ratifying or signing the Convention, making it almost global as a standard in cyber law by August 2025. But other countries such as India at the time refused to join owing to sovereignty reason and non-participation in the drafting process. India has been re-evaluating its position because of the increasing cybercrimes but is still very sensitive to share data with other foreign jurisdictions.[8]

In October 2021, The Convention received another addition in the form of the Second Protocol (2021) to improve the tools of judicial cooperation, such as videoconferencing or joint research team or expedited preservation order, which confirms its position as a foundation in the global law enforcement of cybercrime.

Matters of International Law that are Applicable to Cyber Operations Tallinn Manual (2013 and 2017)

The **Tallinn Manual** is the most authoritative academic project, which examines the application of the current international law to cyber activities, such as cyber warfare and computer attacks that may qualify as armed conflict.

- The 2013 version mainly concerns the cyber operations in armed conflict discussing the application of force, state sovereignty, neutrality and the law of armed conflict principles to the cyber issues.

- The updated version (Tallinn Manual 2.0) which was published in 2017 extends to address peacetime cyber activities including state culpability, cyber spyage, cybercrime, and territorial matters.

The Manual also reminds that the principles of international law, such as the sovereignty and non- intervention should be used in cyberspace to determine how states make the use of cyber incidents and to define where legitimate and legitimate cyber activities take place.

Although the Manual is not legally binding, it educates state practice, judicial case law and treaty talks concerning cyber jurisdiction and cyber conduct, contributing to a normative

[8] F. Spiezia, International Cooperation and Protection of Victims in Cyberspace: Welcoming Protocol II to the Budapest Convention on Cybercrime, 23 ERA FORUM 101 (2022), https://pmc.ncbi.nlm.nih.gov/articles/PMC8978772/

convention at the crossing of cyber actions and international law.

Models of Jurisdiction in Selected Jurisdictions

United States

The computer fraud and abuse act (CFAA) is a major federal law in the US that the country uses and criminalizes unauthorized access and computer intrusion-related activities. The US exercises extraterritorial jurisdiction under the broadest sense of the CFAA, by which foreigners whose codebook hurts US persons or interests can be prosecuted. The case of United States v. is among landmark cases. Ivanov, the rule of effects in the US makes the jurisdiction to apply regardless of the place of origin of the cyber offence. This broad jurisdiction claims US jurisdiction on the cybercrimes committed by global cybercriminals against US services or citizens.

European Union

Using certain tools and methods, such as the General Data Protection Regulation (GDPR), the European Union goes extra-territorial in the protection of information, including cyber-crimes that affect the individuals living on its territory. The GDPR is applicable to any organization that processes the data of EU citizens, irrespective of its location, introducing the model of jurisdiction, which is founded on both effects and links the organization in question with the population of the EU.

Also, the Directive on attacks on information systems of the EU differences cybercrime legislation of member countries and makes it easier to collaborate internationally and uniform jurisdiction.

United Kingdom

Computer Misuse Act (CMA) 1990 of the UK criminalizes the unauthorized access to computer materials and alteration of computer contents and has been complemented by Police and Justice Act 2006. The cross- border application can be ensured since the CMA has territorial jurisdiction through offences being perpetrated against UK computer systems or by the nationals of the UK in another country.

The UK actively joins international cooperation in cybercrime involving agencies such as the Europol and INTERPOL and has bilateral agreements as a means through which they exchange evidence and conduct joint investigations.

The Indian involvement and role in the global cyber law diplomacy

Though India has historically been wary of becoming internationalized in the manner of the adoption of international instruments such as the Budapest Convention because of its sovereignty and data privacy concerns, it has increasingly become active in international cyber law diplomacy:

- India has shown interest in global cooperation systems that agree with its Digital Personal Data Protection Act, 2023 and the Bhartiya Nyaya Sanhita, 2023 standards that provide effective domestic and cross-border prosecution of cybercrimes.

- India is actively involved in multilateral bodies such as the United Nations Office on Drugs and

  Crime (UNODC), the G20 as well as BRICS and is advocating in terms of balanced cyber law models of sovereignty, privacy and achievable reach of jurisdiction.

- It encourages capacity-building efforts, treaties between countries which promote mutual legal assistance, and development of international norms to address cybercrime in common.

Although India is not a signatory of the Budapest Convention, it has bilateral and multilateral partnerships that contribute to strengthening cyber law enforcement and it can be seen that India has a pragmatic strategy to implement a balance between international cooperation and national security.

Cyber Jurisdiction and Cyber Offences JP and Leading Case Laws in India

In India, the judicial precedents have proved quite instrumental in the determination and formulation of the legal boundaries of the cyber jurisdiction and the cyber offences. Since the concept of technology and cybercrime is dynamic, courts have moved to proactively interpret laws such as the Information technology act, 2000 (IT Act), the Indian penal code

(IPC) and recently the Bhartiya Nyaya Sanhita, 2023 as a form of effective reaction to jurisdictional challenges and liabilities of criminals. The legal environment involving the dynamic nature of the legislation that is based on interpretation by the courts in the formation of legislation and laws addressing cyber offences.

Vishnu Datta Sharma and Ors. vs State (1994)

In the case of Vishnu Datta Sharma and Ors. v. State, it was held on the concept of jurisdiction in offences that presence of part constituents of an offence in Indian territory is sufficient to make a claim of the jurisdictional claim, despite other constituents being present in a foreign country. The case was used as the foundation of the principles of extraterritorial jurisdiction accommodated when the BNS adopted Sections 3 and 4 of the IPC in its current form.[9]

The Court noted that any Indian court may exercise jurisdiction over a part of an offence that was committed in India, or the part of an offence that but has effects in India. This is of great importance in cybercrime where the acts (e.g. hacking) and effects (e.g. data theft) may take place across countries in multiple jurisdictions and cause harm wherever that harm is experienced.

Shreya Singhal v. Union of India (2015)

This was a landmark case that was concerned with the challenge of the section 66A of the IT act criminalizing the transmission of offensive messages over the Internet. The Supreme Court invalidated that section (66A) was illegal since it infringed free speech as defined in Article 19(1)(a).

This verdict indicated the importance of having specific and strictly limited cyber laws that do not limit the basic rights in the name of controlling digital crimes. Although not being a case of cyber jurisdiction by itself, Shreya Singhal established new precedents that impose a balance between enforcing cyber offence laws, including the provisions of the BNS, and constitutional freedoms, a necessary judiciary practice in the context of determining whether

[9] Yashwani Goel, Adjudicating and Investigating Cross-Border Cybercrimes: A Study of India's Jurisdictional Framework, 5 INDIAN J. INTEGRATED RES. L. [starting page] (2025), https://ijirl.com/wp-content/uploads/2025/03/ADJUDICATING-AND- INVESTIGATING-CROSS-BORDER-CYBERCRIMES-A-STUDY-OF-INDIAS-JURISDICTIONAL-FRAMEWORK.pdf

to grant jurisdiction in cases involving cyber jurisdiction issues of global effect.

K.S. Puttaswamy (Retd.) v. Union of India (2017)

In the far-reaching ruling that proclaimed the right to privacy a fundamental right safeguarded by the constitution, the Supreme Court transformed the legal domain applicable in cyber offences as well as jurisdictions essentially.

The case has asserted how essential it was to make sure that cyber jurisdiction frameworks, evidence gathering and prosecutions according to such laws as the BNS and the IT Act adhered strictly to privacy and data protection principles. This is very profound when it comes to cross-border data transmission, online monitoring, and prosecution of cyber crimes against personal information where courts have to examine jurisdiction to digital privacy sensitivity.

Avnish Bajaj v. State (2004) -- The Bazee.com Case

In the case of Avnish Bajaj v. Delhi High Court, the court discusses the intermediary liability. State made it clear that it is not the responsibility of digital intermediaries like e-commerce to deal with user-created content nor can they be responsible unless they take no action based on actual knowledge or the court.

As much as the decision shields intermediaries against blanket liability, it equally confirms them as essential factors in cyber offence investigations and enforcement of gun laws such as IT Act and BNS. This body of jurisprudence affects the jurisdiction of cybercrimes, by identifying centers of responsibility in transnational cybercrimes, where digital platforms are situated internationally, but the local users are affected.

State of Madhya Pradesh v. Suresh Kaushal (2001)

The Supreme Court construed the territorial jurisdiction clauses (which currently form BNS 197-199) ratification of the effects doctrine, to mean that offenders may face trial by a court in a place where crimes are caused, even though the crime may have been carried out in a different place. This directly applies in adjudication of cyber crimes in which damages and actions are usually geographically varied.

The Court was keen to remind that jurisdiction is multi-focal and the location of the offence and consequences is important. This made the courts in India have powers to declare jurisdiction over the case of cybercrimes involving servers, victims, or actors across jurisdictions.

Thota Venkateswarlu v. State of Andhra Pradesh (2008)

Expanding on jurisdictional competence, this ruling enlightened procedural issues as to the previous requirements of sanction in investigations of offences committed in the Indian territory but in which there exists nexus with India under the newer laws and provisions which are analogized in BNS.

Such a decision finds special application to extraterritorial cyber crimes, the procedural regularity in the cross-border investigations of cybercrimes and the increased practical enforceability of extraterritorial jurisdiction asserted on cross-border claims of cybercrime under the BNS.

Justice K.S. Puttaswamy Privacy Judgement on the Cyber Jurisdiction

The result of the K.S. Puttaswamy case is still felt in cases of cyber jurisdiction that followed the case as the country must still sign balance national security and data protection and privacy against international cybercrime investigators amid evidence gathering in cyber cases.

Data reduction, use of warrants and proportionality in transnational data access submissions are becoming standard requirements by courts in trials of cybercrime, as influencing the conception of jurisdiction claims and processes under BNS and IT Act structures.

New Judicial strategy towards Cyber Jurisdiction under the BNS

With the introduction of the BNS, courts have started interpreting its implications on consequences-based jurisdiction, digital evidence processing, and web-based organized crime in particular matters of computer worlds. Judicial emphasis lies in:

- Appreciating the multi-jurisdictional aspect of cybercrime.
- The use of effects doctrine in the broadest sense in order to claim jurisdiction over

cyber crimes that cause injury to Indian persons or property.

- Preservation of due process and constitutional rights in the circumstances of violent cybercrime prosecutions.

- Striking a balance between the state interests within the overall jurisdiction and the fairness and privacy.

That intersection between legislative reformation and proactive judicial interpretation promises a new custom-made jurisprudence, one that is fit to 21 st century cybercrime issues.

Difficulties with Determining Online Territorial Jurisdiction

The existence of modern technology which has grown at an astonishing rate and the widespread use of the internet has essentially changed the traditional ideas of territorial jurisdiction in law enforcement concerning crime. Cybercrimes can occur within a digital realm and have no boundaries as compared to physical crimes, which have boundaries and make the jurisdiction complex and controversial in nature. The necessity to determine the proper jurisdiction to use in the investigation and prosecution of digital offences requires an insight into the complex issues involved in cyberspace and the legal reaction.

Anonymity and IP Masking

a. Anonymous Personality in the Internet.

The internet in itself presents the means of anonymity and pseudonymity whereby criminals can hide their identities and escape prosecution. Proxy servers, Virtual Private Networks (VPNs), The Onion Router (TOR) and encrypted communication are some of the techniques used to hide the actual source of digital activity.

b. Influence on attributable effect and felicitous jurisdiction.

IP masking makes it difficult to find the criminal either physically or by using digital methods. The jurisdiction lies in the establishment of the seat of the violator or the violation and masking technology makes it harder to establish jurisdiction or at least start the

investigation. The presence of misattributions may cause the state conflicts, wrongful prosecutions, or loopholes that may be used by the cybercriminals.

c.Enforcement and Evidence Collection Problems.

Cyber offenders are difficult to trace, due to the need of special technical skills and international collaboration to cross the anonymity levels without infringement of privacy rights. Such enforcement challenges are the direct factor in jurisdictional claims, in the situations where the location where the offender was was not the location where the offender was involved.

Data Localization and Cloud Computing

a. Cloud Data is distributed in nature.

Cloud computing prevents data and processes by making use of globally dispersed servers without a definite place of presence. The data that is relevant to a single crime might be stored in two or even more jurisdictions.

b. Jurisdictional Ambiguity

In the case of decentralized data, it is not easy to claim control over storage or processing servers. As an example, the identical data can physically reside in servers in various countries and each has claimed jurisdiction and applied conflicting laws.

c. Laws of localisation of Data and their impacts.

Data localization requirements in different countries have placed the requirements on the storage of some data within a country with the aim of having control over the data through regulation e.g. the pending data localization requirements in India in the Digital Personal Data Protection Act. Although the laws aim to enhance the control of the jurisdictions, they result in disintegration, higher costs of compliance, and the possibility of conflict between the multinational cloud providers and the new laws.

International Armed Confrontation

a. Conflicting Cyber Laws and Jurisdictional Statements.

The law on cyber embraced by different countries is different, and as such, similar or jurisdictional clashes may be placed on the same action. An example of this is the fact that a particular country will criminalize a particular online speech as sedition whereas another country will consider it to be a free speech.

b. Incompatibilities in Data Protection and Privacy Standards.

Differences in privacy legislation are barriers to transnational data exchange in investigations, which are needed in the process of prosecuting cybercrimes. The mutual assistance is complicated due to differences between GDPR and other jurisdictions.

c) International Cyber Cooperation Effect.

Cybercriminals are using exploitation of loopholes and shopping of jurisdiction as a way to thwart legal assistance or extradition under the pretext of cooperation that is required in the case of the use of Mutual Legal Assistance Treaties (MLATs) or extradition.

Problems of Enforcement: Mutual Legal Assistance and Extradition

a. Complications in the Processes of MLATs

MLAT processes may be tedious, bureaucratic and rely upon mutually beneficial cooperation. The high pace of cybercrimes requires prompt reaction, which is not possible with the conventional MLAT models.

b. Challenges in Extradition

The extradition of cybercriminals is a highly delicate matter of diplomacy, legal differences, and the political factor. The lack of extradition treaties or unequal cases will result in the fact that offenders who act on the cross-border basis will be impunished.

c. Disputes on Jurisdiction Stalling Implementation.

The problem of parallel prosecutions in other jurisdictions or conflicting orders leads to paralysis of the enforcement, which negatively affects the fight against cybercrime in a global-level.

Problems of Admissibility and Collection of Digital Evidence

a. Complexity and Nature of Digital Evidence

Electronic evidence is unstable, immeasurable, and can be easily distorted. Special forensic methodologies are needed in collection and preservation in order to achieve reliability.

b. Admissibility and Standards of Law.

The admissibility of digital evidence by various jurisdictions differs thereby influencing cross-border prosecutions. Issues of chain of custody, authentication and integrity are imperative.

c. Sharing of Evidence of Different jurisdictions.

Efficient international exchange of digital evidence is hindered by legal, technical and procedural impediments. Variables on privacy laws and data protection also complicate and hinder evidence transfer.

d. Technological factors and Capacity constraints.

Absence of trained staff, inadequate forensic infrastructure, and technical loopholes do not allow to be handled with proper evidence processing, undermining the success of prosecutors and their jurisdiction discussions.

Digital Territorial Jurisdiction Recommendations and Way Forward

The accelerating development of digital technologies, and the complexity of cyber crimes imply the essential problems with the traditional territorial jurisdiction. The Indian legal system, which is still in a process of being reshaped by the Bharatiya Nyaya Sanhita (BNS), Information Technology Act (IT Act) and similar laws, must be constantly improved in order to address these challenges efficiently. This part gives specific, systematic suggestions of how to bring a number of legal, procedural, and technological loopholes that stifle effective and executable digital territorial jurisdiction.

Knowledge Requirement of Special Cyber Jurisdiction Causes During BNS

The BNS has updated India penal code but can go further by having clear cyber jurisdiction

clauses that:

- Specify lawfully the place of commission of cyber offences considering the complexity of the distributed digital actions and outcomes.
- Indicate jurisdictional precedence where a crime is interstate- Turkey, an offence regarding a house is committed where the data was stored or accessed and altered, or where the harm was inflicted on the victims.
- Expound jurisdiction regulations on cybercrime syndicates across nations, information breaches and online fraud.
- Give specifications on how Indian courts should assert jurisdiction over harm inflicted within India even though the perpetrator is not found in India, and the doctrine of strengthening effects was applied.

Clear provisions have been stipulated by statute, which will minimize jurisdiction litigation, merge prosecutors and ensure that courts can effortlessly have jurisdiction.

- Crimes yet does not contain substantive provision of extensive penalities.
- The BNS is a substantive incorporation of cybercrime that must explain how its procedures overlap with the provisions of the IT Act.
- Balancing the two acts through the formation of cross references, similar definitions, mutual enforcement provisions and common guidelines to the prosecutors would ensure no duplication and conflicting mandate.
- Coherence can be provided by the creation of a joint working group of legislators, cyber law.

  specialists, and judicial administrators to oversee, revamp and harmonize provisions on a regular basis.
- The legal practitioners should be equipped with the appropriate knowledge of the statutes by training programs and judicial capacity building.

This synergistic relationship will monitor a smooth criminal art of the procedures in adjudging cybercrime.

India needed to become a member of Budapest Convention on Global Cooperation

The failure of India to ratify the Budapest Convention on abetted crime restricts the entry to formalized global collaboration tools that could be important in international investigations:

- The most important international tool to expedited mutual legal assistance, information, and coordinated enforcement is the Budapest Convention, which allows the signatories to do this.
- Becoming part of the Convention would help extend India the capabilities to promptly acquire and share electronic evidence, extradite cybercriminals and work with multinational enquiries, essential against fleeting and international cyber stressors.
- Even though India has sovereignty and data privacy issues, these can be solved with proper accession-related declarations and ensure its privacy.
- This active activity demonstrates India's adherence to the international cyber standards, which enhances bilateral and multilateral relations on cybersecurity.
- An integrated accession approach including far-reaching consultations with the parliament and stakeholders can make the way to signature and even ratification.

Becoming a member of the Budapest Convention would be elective in enhancing the capacity of India to enforce a jurisdictional UN network with regard to cyber-related issues.

Technical Expertise in development of Cyber Crime Courts

Complicated nature of cybercrimes requires special legal apparatus:

- Create special Cyber Crime Courts/ Benches with judges who are trained in cyber law, digital evidence and other matters that concern technology.
- Continued legal education and technological up to date of the judges and prosecutors

to be effective in handling cases relating to cyber.

- Implement the digital format of the courtrooms which will allow the safe presentation of evidence, the implementation of digital forensics, and the assistance of expert testimony.

- Facilitate process change; provide the ability to have expedited proceedings of cyber offences to minimize delays in judicial procedures, and increase victim trust.

- Promote multidisciplinary collaboration between the law enforcement, cyber experts, data privacy commissioners, and the judiciary in the field of cyber justice.

This type of specialized court plays a critical role in efficient resolution of complicated cybercrimes in the Indian legal process.

Powering up Digital Forensics and Cross-boundary Data-Sharing Contracts

A good prosecution and jurisdiction depends upon well-developed digital forensics and cooperation with other countries:

- Make a heavy investment into the construction of state-of-the-art forensic laboratories and staff them with qualified professionals who would be able to process sophisticated cybercrime evidence and cryptographic data.

- Establish national cyber forensic coordination agencies working in coordination with district and

  state law enforcement to provide uniform evidence ingesting and preservation.

- Discuss and sign bilateral and multilateral data-sharing agreements that allow rapid decision- making on transparency of digital evidence that meets the privacy laws of the respective countries.

- MLAT procedures related specifically to cybercrime are streamlined in order to minimize delays during procedures.

- Standardized methods of admissibility of cross-border evidence and chain custody

in accordance with the best international practices and the Bharatiya Sakshya Adhiniyam.

- Encourage the use of cloud and telecommunication providers in partnership with the government to create a legal entry to data when it is necessary within the investigation so that time loss is minimal.

This ability increase is crucial in asserting control and administering justice on transnational cyber crimes.

Cyber Offences -Legislative Understanding on Place of Commission

This is because a fundamental issue that has always existed is the lack of clarity on where a cyber offence is considered to have occurred:

- There is need to clarify in the legislation the distinction between the place of act (where the offender actually acts) and the place of effect (where the impact of the crime is experienced).

- The law should acknowledge cyber crimes as possible crimes in a range of jurisdictions since digital crimes are virtual and are distributed.

- The laws of India, especially of BNS, ought to establish regulations of jurisdiction in cases where data stored in foreign servers is accessed or damaged in India.

- Facilitation of joint jurisdiction of courts making joint jurisdiction possible so that there could be cooperation or deference between jurisdictions to prevent the resulting invincibility.

- Clarity of language in legislation will minimize litigative uncertainty and allow prosecutors sufficient to exercise their jurisdiction as per territorial law in criminal offenses that happen digitally.

Conclusion

During modern digital age, the very idea of the territorial jurisdiction is seriously changing.

The traditional paradigm that was based on geographical borders that existed in the physical was now faced with the dynamic and boundaryless character of the cyberspace. Digital territoriality provokes the sovereignty principle because cyber offenses have the tendency of breaking the borders of nation-states immediately and include actors, servers, and victims spread around the world. The introduction of cloud computing, anonymity technologies, and the complicated data flows all heighten the nettlesome of identifying the locus of online crimes that forces authorities all over the world and India as the digital economy to re-think the jurisdictional systems. In this regard, the concept of territorial jurisdiction is being interpreted more as a locality in space not as a spatial locale, but as a network of exchangeable and multi-faceted points of contact with the place of act, place of effect and the place of impact.