WWW.IJRPR.COM

International Journal of Research Publication and Reviews

Journal homepage: www.ijrpr.com ISSN 2582-7421

JURISDICTIONAL CHALLENGES IN REGULATING CROSS-BORDER OFFENCES FACILITATED THROUGH DARK-WEB MARKETPLACES; A LEGAL ANALYSIS

Thanu Varshini Naaharajan

Sastra deemed University

ABSTRACT :

Cybercrimes no longer need to be confined to a geographical location as digital infrastructure is spreading around the entire globe. The dark web has become an enormous threat, as criminals are able to do business underground and out of the way of local law enforcement officials. They use multiple layers of encryption and transfer monetary funds and data almost untraceably. The pursuit and prosecution of these criminals and their legal liability have turned into a real nightmare for police and crime authorities everywhere.

Much is known about the technology of anonymous networks, such as Tor and how it works, but most scholarship presentations gloss over the actual legal trouble: jurisdiction. How does a crime that goes on to impact one, two, three or four countries become a reality? You have criminals in one country, victims in another, servers somewhere else, different clouds and data storage in yet another. The selection of a country to prosecute, is more a question of a puzzle, than the reading of a statute book.

This study uncovers that muckraking. It highlights the lacunae in India's laws, in particular Section 75 of the Information Technology Act, 2000, and international legal treaties, in a world in which offences seamlessly cross borders. The study deconstructs the case law, statutes and treaties to identify groundbreaking shortcomings in the existing system. It ends with few clear recommendations about legal changes to enable law enforcement to do its job without trampled-on foreign sovereignty.

Background, Introduction, and Significance

Yes, the digital revolution provided us with unfettering communication and how the world does business; there is a dark side to the convenience. Now, criminals can work without passports, which are not subject to any specific state's laws. In particular, the dark web provides an environment where any number of markets for illicit activity can be originated and which is only accessible to special software such as Tor. Websites such as Ahmia have indexed directories for web content that can be browsed, while regular users may be looking for privacy with a browser like Brave, criminals are likewise buying and selling goods without ever coming up for air.

In the meantime, these platforms enable criminals to operate and co-ordinate from any corner of the world. A transaction could involve the buyer being in India, the server being in Singapore, the marketplace being operated in Russia and evidence being stored in a cloud in the U.S. It was chaos, everyone and everything was in disarray. Completely upends the traditional notion that a crime occurs in one location and should be prosecuted in that location.

In this research we focus on India's laws, whether they are equipped to address cross-border crimes. It is closely focused on how Tor is able to hide users, how cryptocurrencies complicate things and why local cops are, in many cases, helpless as they face off against criminals who never set foot in India, but aim to target its digital infrastructure. There's a lot of computer science research going around, but this paper focuses on the legal issue, rather than the technical issue.

Without international co-operation nothing changes. India's only chance for capturing these offenders is to rely on assistance from foreign agencies for data, evidence, or arrest warrants which can only dribble down through feeble and inefficient legal processes. This paper does not only examine the statutes, but clarifies how Indian jurisdiction, international sovereignty and cross-border assistance actually work out on the ground.

Literature Review

Matthew Robert Shillito, Untangling the 'Dark Web'

Shillito explores the ways that on the dark-web networks virtually discard all of the traditional criminal law assumptions regarding boundaries. Offender

and victim, digital evidence, money all are distributed internationally, rendering territorial law virtually unhelpful, he says. He also demonstrates that when tech is anonymized, the police aren't quite at the same level, and struggles to deal with legal protocols designed for a simpler era. His analysis doesn't go into any detail of the law of a country, this current study continues there and examines India and its capacity to address the issue.

Ahmed Ghappour, Searching Places Unknown
Ghappour explains how law enforcement is compelled to dust off the hacking tools when it's time to break out of traditional tracking methods. However, when agencies lack an idea of where the target is until they have infiltrated a computer, they are fast heading into territories of other nations, leading to diplomatic wrangling. The crux? Paper power legal authority does not equal real world power - the power to investigate, arrest or collect evidence overseas. The tension is not just in the U.S. but also in India, particularly under the IT Act and the new Bharatiya Nyaya Sanhita, as Ghappour said his focus is the U.S.

Paul Arnell & Bukola Faturoti, The prosecution of cybercrime why transnational and extraterritorial jurisdiction should be resisted
These authors cry foul at the push to continue to extend cybercrime legislation beyond the borders. Cyber offenses are continuing to grow around the world, despite more legislation. They say that ever-expanding jurisdiction creates more issues, breeds conflict between nations and is often unresponsive on the ground. Instead they advocate revising regulations locally, not throwing the ever-broadening net. This research does take their warning seriously, and does not see extraterritoriality as the solution to everything, but rather as having some definite boundaries.

Paul De Hert, Cihan Parlar & Juraj Sajfert, The Cybercrime Convention Committee's 2017 Guidance Note on Production Orders
In this article the Budapest Convention approach to international evidence collection is under scrutiny. The authors would point to the unilateral demands for electronic records that raise issues of sovereignty and skirt over fundamental notions of privacy rights. They emphasize that criminalisation by a state does not imply that foreign tech companies have to be obliged to comply or provide suspect data. These are obstacles that are foremost in Indian investigators' minds as they pursue evidence on foreign servers.

David Wicki-Birchler, The Budapest Convention and the General Data Protection Regulation
Wicki-Birchler discusses the conflict between the Budapest Convention and the European Union's GDPR, which works in contrast while the other looks to enhance international police partnerships. All of these conflicting priorities must be considered with each cross-border investigation. This is significant for India because any attempt of a meaningful crackdown on the crimes in the dark web falls under the ambit of foreign data-protection laws and individual rights all of which are considered by this Study in its proposed legal changes.

Research Gap

The same basic issues are cited in most scholarships: borderless crimes make jurisdiction difficult, markets are localized on the dark-web and collecting data abroad is nearly impossible. However, surprisingly, there is not much research which examines how Section 75 of the IT Act and new provisions under the BNS hold up India specially, to these challenges. This study fills that gap by directly comparing the claims of what Indian law can achieve and what it can actually enforce with the players or the proof not being within India.

Statement of the Research Problem

Dark-web marketplaces divide up each aspect of an offense: the criminal, the victim, the servers, the evidence all may end up in separate countries. This fact undermines traditional concepts of jurisdiction. Indian law, as specified in Section 75 of the IT Act and Section 1(5)(c) of the BNS, states that it can go after crimes being committed against Indian computer resources, no matter where the perpetrator is. The problem is that paper and ink creates power, but in practice it's not as easy as people might think. Sovereignty boundaries are a hindrance to real world investigations. Indian police authorities are not allowed to simply confiscate servers and/or servers located outside the country or arrest a fugitive in another country without getting entangled in the conflicting dynamic of slow, uncertain and occasionally nonexistent mutual assistance treaties. In attempting to do so, another form of violation of international norms and basic rights may be attempted.

Thus, the research problem here will be evident: while Indian law makes considerable forays into extra-territorial jurisdiction, its ability to enforce those claims in the face of cross-border darknet offenses is dauntingly impractical. This paper dissects the worst offenders of that friction, and outlines possibilities for reform consistent with foreign sovereignty and due process.

Research Objectives

This study wants to test just how far India's extraterritorial cyber laws can stretch.
The goals are:

- Unravel digital jurisdiction see how the meaning of jurisdiction shifts in a world where crimes cross new borders every day.
- Test the IT Act's real-world power, especially Section 75.
- Investigate how the BNS extends penal law to cases that start abroad but target Indian systems.
- Draw the line between writing tough laws and truly being able to investigate and prosecute under them.

- Identify the hurdles Indian police face in securing evidence from overseas providers.
- Examine whether mutual legal assistance and international police networks actually work.
- Catch the loopholes that let offenders slip through.
- Propose reforms that give Indian law teeth against darknet crimes without trampling over other countries' rights or due process.

Research Questions

This study focuses on some tricky legal questions about transnational cybercrimes:

- Can Indian courts actually claim criminal jurisdiction over dark-web offenses when the main culprit sits outside the country?
- How does Section 75 of the Information Technology Act, 2000 really work when a darknet crime involves a computer physically inside India?
- What's the unique legal effect of Section 1(5)(c) of the Bharatiya Nyaya Sanhita (BNS), 2023, for cybercrimes carried out abroad but aimed at Indian systems?
- Does having extra-territorial jurisdiction in law give Indian police real power to investigate suspects or seize evidence in other countries?
- What sovereignty conflicts or enforcement headaches pop up when key digital evidence for an Indian dark-web case sits on servers overseas?
- Are current mutual legal assistance treaties and international police collaborations actually helping bridge the enforcement gap for borderless dark-web crimes?
- Which statutory tweaks and procedural changes could help Indian cyber jurisdiction work better without overstepping on foreign sovereignty or global legal norms?

Scope and Limitations of the Study

Scope

This research does not delve into the technology. Rather, it explores the workings of jurisdiction in the case of dark web criminal incidents. It's a question of who has the "legal" authority to address these crimes and the practical application of that authority.
The study covers:

- The clash between traditional borders and expanding extra-territorial rules.
- Where Section 75 of the IT Act hits its limits when crimes happen outside India.
- How the BNS applies extra-territorial criminal liability.
- New rules under the BNSS (2023) for international digital investigations and data collection.
- How to manage investigations that stretch across several countries.
- The obstacles in retrieving and authenticating electronic evidence stored under other countries' laws.
- How well international legal frameworks and cooperation treaties work.
- The constitutional arguments about sovereignty and overlapping jurisdictions.
- A critical review of major Indian and global court cases that set these borderless rules.

For clarification, this article's study is on the dark web, which is merely a more online environment in which these legal battles take place as a backdrop. Things such as onion routing and complete user anonymity are only explored to the extent that they make jurisdiction difficult.

Limitations

- Doctrinal Only: All of the research conducted here is doctrinal from statutes, court decisions, treaties and literature. The sense of "on the ground" information from police, prosecutors or cybersecurity experts is missing, and it fails to give a sense of what is really being done on a day-to-day basis.
- Structural Focus: The paper does not disaggregate individual types of darknet crime (narcotics, fraud, trafficking etc). It's simply regarding the legal structures that encompass them en masse.
- Tech Moves Faster Than Law: New cryptographic tools and changes occur much more rapidly than lawmaking. The information included herein may become outdated in the future due to changes in technology and legislation.

Research Methodology

1. Research Design

The study draws primarily upon doctrinal legal analysis with selective comparative analysis, where the analysis of other countries is helpful for India's context. The most evidence is being found in carefully reading the statutes and judicial decisions, and then making some deliberate comparisons.

2. Sources of Data

It's all documentary:

- Primary: IT Act (2000), BNS (2023), BNSS (2023), relevant court decisions, international treaties.

- Secondary: Peer-reviewed journals, textbooks, scholarly critiques, institutional reviews, whitepapers on transnational cybercrime.

3. Technique of Data Collection

The information is based on intensive reading and research of legislation and judgements. Academic articles are selected from well-known legal databases. The study is based on at least five peer-reviewed papers concerning such matters as darknet liability, cross-border jurisdiction, evidence preservation and international policing.

4. Technique of Analysis

The materials get examined by:

- Statutory Interpretation: Scanning the exact language of Indian laws about internet crimes.
- Case-Law Analysis: Looking at how courts reason through physical vs. digital jurisdiction fights.
- Conceptual Mapping: Testing classical jurisdiction doctrines territoriality, nationality, effects-based.
- Comparative Assessment: Studying global models for cross-border internet policing.
- Gap Analysis: Finding the gap between India's legal power and its actual enforcement muscle abroad.

Legal Interpretation

It's a study that compares legal structures to the unruly nature of trans-border crimes in the dark-net. The prime objective is to test whether India's new criminal laws (such as Section 113 of the BNSS for requests for 'information') even cover situations where the suspect, network and data are not within the boundaries of India.

Introduction to Dark Web Marketplaces and Jurisdiction

The Darknet Environment and Crypto Marketplaces

You need to understand a lot about the dark Web in order to understand these cross-border crimes. It's a secret part of the web that can only be accessed using instruments of anonymity such as Tor. There are pages for buyers, sellers offer their wares, there are buyer ratings, there are automated dispute systems, and it's as close to a real ecommerce marketplace as you can get!

But, they are selling drugs, weapons, stolen data, malware, pretty much anything which is considered contraband. Anonymity is built-in. Hidden services are services that hide the location of their servers, onion routing (removes IP traces). One single deal may have a seller, a buyer, a server and the crypto payments routed all over the world. That's why the dark web is more of a tech conundrum than a legal one.

The Doctrine of Digital Jurisdiction

Since these operations ignore borders, traditional legal models get strained. This study breaks "jurisdiction" into:

- Territorial: Authority grounded in crimes committed on a country's soil or causing harm there.
- Extra-territorial: Legal reach over crimes done abroad usually tied to the perpetrator's nationality or national security effects.
- Prescriptive: Power to create laws and decide what borderless behavior falls under national codes.
- Adjudicative: Courts' power to hear cases, interpret statutes, and deliver verdicts.
- Enforcement: Power to investigate, issue warrants, make arrests the most limited piece under international law.

Research Boundaries and Framing

This study does not account for server protocols or encryption if they do not affect the geographic aspects of a host, a suspect or a data trail. The chapter is useful to analyse the nature of the legal battle and to examine the India's evidence collection, mutual assistance, BNS, and IT Act.

Indian Legal Framework Governing Cross-Border Cyber Offences

Section 75 of the IT Act: The Overbroad Nexus

The provision of Section 75 is the primary provision of India for providing extra territorial jurisdiction over cyber space. It extends beyond the borders of India and is applicable to any crimes committed anywhere where a computer system is in India.

How the courts will interpret "involves" is the key in dark-web investigations. The strict interpretation would be that there must be evidence of intentional efforts to target an Indian resource. A loose interpretation would mean that jurisdiction kicks in at any point where the operation played with the internet's backbones in India, either in the form of a routing server, a victim's smart phone, the ISP node, etc.

As it's a global traffic, which is really split among all the nodes, this interpretation defines just how much crime Indian courts can claim. Take the case of Section 75 - even if it does provide authority, overcoming anonymity and bringing foreign criminals to Indian courts is the classic formula for disconnect between what the law allows and what is enforced.

Section 1(5)(c) of the BNS, 2023: The Targeted Approach

In the BNS, the penal code has been extended to apply to any person outside India who commits an offence against an Indian computer resource as

indicated in section 1(5)(c). Offense should be something which is punishable under BNS, in case of any offense in India.

A significant difference between BNS 1(5)(c) and Section 75 of the IT Act can be seen. Section 75 is wider as it applies when a crime "involves" an Indian digital asset. BNS requests further evidence of "targeted" asset. To show that there was targeting in the complex darknet transaction is a more difficult hurdle to jump than merely involvement.

Section 208 of the BNSS, 2023: Procedural Loophole

But IT Act and BNS provide extra-territorial liability while procedure is under Section 208 of BNSS (corresponding to the old Section 188 CrPC). This is because under Section 208, offences committed outside India may be tried as if they have occurred in India, but only with the previous sanction of the Central Government.

The catch? Under Section 208 only an Indian citizen who is outside the country and foreigners whose ships or aircraft are under Indian registry are covered. Does not explicitly mention foreign nationals involved in running the operations of the dark-web in India. That leaves them with a tangled situation: If a foreign darknet mastermind is arrested, is it possible to conduct the trial without Central's approval, or will the process fail because of the loophole? This gap is important to appreciate to begin seeing where India's grand internet policies run amok into old procedural hurdles.

Judicial Approach to Cyber and Extra-Territorial Jurisdiction

1. The Doctrine of Continuing Offenses: Ajay Agarwal v. Union of India

For an insight into the approach of Indian courts in dealing with cross-border offences, refer to Ajay Agarwal v. Union of India (1993) 3 SCC 609. This was a conspiracy case of cheating an Indian bank with some of the activities being done in Chandigarh, some in Dubai and some in India. Criminal conspiracy is a "continuing offense," said the Supreme Court. It is found in any place a co-conspirator is doing or does anything to further the scheme. Key takeaway: Location of the crime/effects is more important than citizen/residence of accused. Therefore, if it is a darknet transaction that causes harm in India, then Indian courts can attempt to address it locally, it's not, "extra-territorial." Furthermore, the case concerned the old case the 'prior sanction rule' which was the precursor to Section 208 BNSS. Although the case pre-dates the current era of cryptography, the case still raises points of fundamental law.

2. The Principle of Purposeful Availment: Banyan Tree Holdings

The criminal continuity principle is set by Ajay Agarwal whereas digital civil cases throw light on the boundaries of jurisdiction. In Banyan Tree Holding (P) Ltd. v A. Murali Krishna Reddy (Delhi HC, 2010), the controversy was regarding IP, where neither of them was residing in Delhi. Plaintiff sought jurisdiction on the ground that it was accessible in Delhi.

This was rejected by the High Court. Even for long-arm jurisdiction they said that just being accessible is not enough, but the defendant must have a "purposeful targeting" of the local forum. Using the "effects test" you have to establish that actual harm occurred within the territory. Aside from the fact that these digital jurisdiction standards particularly the balance between Banyan Tree's more restrictive model and the worryingly more expansive WWE case-are presently up for review by a constitutional bench. However, purposeful availment is still convincing but not finally decided in case of borderless networks!

3. Comparative Application to Darknet Marketplaces

With respect to jurisdiction, there is no mistaking it - just because an opening can be made up from a mobile phone in India doesn't mean India has any hold on the dark-web marketplace. Accessibility is not the law of the land. Rather, prosecutors must be able to come up with a good "connecting factor," that is, something tangible to bind the crime with India.

That's why this research asks if Indian jurisdiction should really depend on more specific details, like:

- Where the hacked computer sits.
- If the victim or the scammed entity is inside India.
- The nationality of whoever's running the darknet platform.
- Where the illegal code or transaction actually started.
- If the crime caused real social or economic damage in India.
- Whether the offender clearly aimed their actions at Indian people or networks.
- Which territory holds the most important digital evidence.

In practice, these are the factors which Courts apply to determine the question whether a case truly "involves" India as per the words of Section 75 of the IT Act or whether some targeted action has been undertaken as per Section 1(5)(c) of the BNS, 2023.

Cross-Border Enforcement and Digital Evidence

The Operational Split: Prescriptive vs. Enforcement Jurisdiction

Here lies the watershed: while it is true that India makes laws that declare what offences are crimes even when committed in other countries, Indian police can't necessarily enforce those laws in other countries. More than one person has the right to say that something is wrong and illegal, but not the power to actually do something about it.

Thus, if a dark-web crime includes, for instance, one villager in Country A, another in Country B, servers in Country C and a victim in India, then, technically, Indian law applies to the victim's side of the crime. However in reality Indian investigators can't waltz into the other countries, grab servers or make arrests without going through mountains of diplomatic hoops. As a result, there is this enormous disconnect: Indian courts go on declaring that they have jurisdiction but to make anything happen is a grind.

The Forensic Bottleneck of Overseas Digital Evidence

Things are worse if the evidence is kept outside the United States. Conventional legal processes are of limited assistance when the data required is on server in another country. 99% of time, India is waiting for replies to Mutual Legal Assistance Treaties (MLATs) or the correspondence sent via Embassies which usually take forever. Despite entering into dozens of MLATs, Indian police typically receive evidence from sluggish and formal procedures. In recent times, whose involvement with other countries has been outlined under Sections 112 and 113 of the BNSS, 2023, and the Ministry of Home Affairs serves as the liaison for US big tech companies. The US will also typically require additional documentation, such as "probable cause" in order to give anything to them, and this further slows down the process.

An MLAT process can last for 10 months and is not unusual. By that time, logs and data could have been deleted and/or overwritten and may never come into the possession of Indian police.

Multilateral choices don't actually assist an awful lot, either. Due to concern of sovereignty and cross-border data grabs, India has never signed up to the Budapest Convention on Cybercrime. The ambience regarding its standing under the new UN treaty is still unclear and for the time being, India flutters in a way of a piecemeal arrangement of one-on-one treaties.

The Five-Stage Framework of Digital Accountability

To make sense of all this, here's how you break down a cross-border cybercrime case:

1. Does Indian law even apply to what happened overseas?
2. Can Indian courts actually try the case?
3. Can Indian police do any real investigating, and where?
4. Can they collect, prove, and use evidence from another country in an Indian court?
5. And, finally, can they force someone overseas to face consequences like extraditing a fugitive or freezing assets?

International Cooperation and Jurisdictional Conflicts

The Budapest Convention Framework and Structural Limitations

Each individual country will not be able to combat global darknet crimes alone. The servers, culprits and money trails are continually crossing the borders. Hence the need for cooperation between the countries.

Budapest Convention is the most comprehensive framework treaty on cross-border cybercrime. Sets a course for data sorting, evidence retention and cooperation building. It has even been enhanced over the years to allow police to directly contact overseas tech providers. However, India has stayed out, primarily due to Article 32, which allows countries to access data on Indian servers without complete permission in India a major issue in terms of sovereignty for India. Thus, India is continuing to use diplomatic avenues which are slower.

The Evolving United Nations Architecture: The Hanoi Framework

UN developed its own cybercrime convention in response to the gaps in the regional treaties. It will remain open for signatures until the end of 2026, and will enter into force upon the ratification by 40 countries. It's a significant change but, in September 2026, India finally signed and signing is not the same as enforcing. It has yet to pass and implement domestic legislations that will count in courts. Well, the treaty remains on the back burner, for now.

Direct Executive Pacts, Sovereignty Tensions, and Overlapping Claims

In the interim, nations are negotiating quicker and direct deals such as via the US CLOUD Act, which not only fast-tracks data requests for Indian police but also does so without the need to wait for MLAT.

All these new cross-border tools have one certain issue in common: how to maintain speedy access to data whilst taking account of the sovereignty of other countries, and the right to privacy of individuals. Abuses and political snooping are the greater the more unilateral power countries acquire. Indeed, it was these issues that led to the impasse during most of the UN treaty negotiations.

With darknet markets, it gets even dicier. Sometimes, three or four countries may argue that they are the ones that should take action for prosecution, as the victim, the server and the perpetrator are all located in different countries. Right now there is no system in place to determine who has the lead, and cases end up being bogged down in several prosecutions and extradition battles.

Eventually, more and more "long arm" legislation will not solve the issue. The only true way forward is to create shared, rapid and mutually beneficial cooperation with robust protection of human rights and privacy.

Findings and Conclusion

Synthesis of the Jurisdictional Paradox

This research reveals that courts have all such theoretical powers in order to cover the cybercrimes on paper in the Indian law. However, implementing those laws in real world, international, cases is another matter. Many hurdles can lie between "we have jurisdiction" and "we have evidence and a conviction," particularly in the case of dark-web marketplaces that make everything more difficult to trace.

Core Legal and Procedural Findings

- Section 75 of the IT Act is the key provision of the Indian law against fighting cybercrime originating from other countries. The catch? There are two ways of reading this word "involves", either narrowly (involves specifically India) or broadly (does any trade traffic happen through India). The usefulness of the section is in the minds of the judges reading it.
- The new BNS, in Section 1(5)(c) for the year 2023, empowers the prosecution to act against the foreigner targeted to Indian networks as the language in the BNS is more stringent on evidence than the IT Act.
- Whereas police power is different from the legal jurisdiction. Indian police do not have the ability to arrest or seize servers outside of the country if foreign authorities do not "play ball." All of the communication is done through diplomatic channels for the most part, old-fashioned MLATs and formal letters. But even India signing the UN cybercrime treaty hasn't accelerated things; the treaty is yet to be ratified and thus become active.
- The next hurdle is surmounting the issue of admissibility. According to Section 63 of the BSA (2023), you have to submit a locally signed certificate to allow digital evidence. Yet, when key evidence is on an American or European server, how do you show that the evidence is legit? Foreign-cloud data is still in limbo, since the law doesn't specify.
- The technical tricks that are used on the dark-web, in conjunction with its routing methods through Tor, make it almost impossible to attribute. Police can hardly even determine the location of the servers, let alone suspects. Advances in crypto tracing and Open Intelligence Sharing is the only way investigations can work.

Conclusion

Thus, rather than adding to the layer of extraterritorial laws, sound, direct, and expeditious information-sharing agreements ones that respect privacy and accommodate modern evidence certification processes are the true solutions.

Recommendations

The research points to six targeted reforms. Here are the top two:

- **Formulation of Clearer Procedural Guidance:** Indian laws are general but there are no clear instructions for the people on the ground, particularly when it comes to suspects or information located outside India. The Ministry of Home Affairs should collaborate with cyber law experts for the issue of a clear official Handbook. The guide should define in detail how to make requests to foreign countries, how each of the requesters is responsible for what, and what documents foreign states and tech companies require. Investigators will not waste valuable time and argue technicalities with better procedures.
- **Streamlining and Strengthening International Cooperation:** Today the MLAT and court-letter procedures are slow and effectively compromise all expedient investigations in fast-paced, encrypted digital markets. These systems should be put online, standard Requests for Digital Evidence used, and real time linkages established with overseas agencies in India. With more and more treaties (such as the UN Convention) being in force, India needs to catch up, scrap red-tape, negotiate executive understandings to facilitate faster data requests and start preparing its institutions to make faster cooperation happen on the ground.
- **Setting Up Specialized Investigation Teams:** Investigating what goes on in the darknet is not only tricky, its a race against time and most regular police teams are not a combination of tech skills and legal expertise! This is largely the reason why India should have separate cyber-investigation teams that have individuals from various backgrounds. Simply put, computer forensics experts in the same room as international law prosecutors makes it easier to determine where servers are housed, how data bounces from one country to the next and where the optimal avenue for collaboration lies. Quick footwork on these steps is essential to bring in any evidence in time before it is lost forever.
- **Clearly Defining Enforcement Boundaries:** With respect to "international investigations," it's no secret that these investigations can become a diplomatic headache. Indian laws and institutions should unequivocally state that the fact that India has the legal power to extend its jurisdiction to a foreign country, does not imply they are empowered to take any unilateral action in a sovereign nation. Strong arm tactics like anything from a remote search to the mirroring of foreign servers or grabbing data from a foreign site must have the foreign country's permission or, at least, a treaty. By laying it down in law, India's strong position on digital sovereignty is not only ensured but also helps

forestall conflicts with other countries and the risk of loss of essential evidence in courts because of wrongful gathering.

- **Fast-Track Measures for Digital Evidence Preservation:** Dark web electronic evidence can disappear rapidly, from routing logs to crypto-wallet data to user accounts-before any formal request for legal support even makes it through the system. Therefore, India must make it simpler to take swift action. The legislation should permit authorities to immediately request foreign service providers to freeze certain key metadata while the broader legal request is muddling through the diplomatic morass. However, following the model of the Budapest Convention, the preservation of urgent data should not be tied to production of evidence, as such preservation may result in the loss of evidence if it goes beyond that.
- **Procedural Rights and Safeguards:** The increased ability for Indian agencies to investigate abroad isn't merely a technical or legal solution; it carries with it the risk of governmental overreach, if the necessary safeguards are not established. Prisoners, like everyone else, have a right to privacy, due process and sovereignty as established in India's own constitution. Whereas, if other nations are going ahead and providing greater investigative powers, India has to consistently balance more investigative powers with two factors: Judicial oversight and defining rules on when and how electronic evidence can be sought. All requests for digital evidence must undergo a necessity and proportionality test; and there are clear guidelines as to what should happen to such evidence once it is acquired.

Conclusion

With misplaced ideas of territory and jurisdiction, dark web marketplaces now dominate the ground. Old rules presume you can deduce the where, who, what and who was hurt. The dark web dispels those myths: servers may be in one country; networks that hide the users may be in a different country; the admin of a particular site may be in a third, the victims may be in India, and the evidence may be hosted somewhere else. Now it's not clear who the data belongs to which country can do the investigation, prosecution, or require it.

The fight is not unrecognized by the Indian law. If a computer or network is involved in a crime, then the Information Technology Act, 2000 can be applied anywhere (Section 75). The opportunity to cheat Indian resources means the same per the Bharatiya Nyaya Sanhita, 2023. The Indian courts are also not averse to adjudication of cross-border crimes with a definite nexus in India - but you do need more than just a website being available in India.

Nevertheless, these rights may not always be the same as the realities. What if the suspect or critical elements of the case are abroad? An Indian court may be able to hear the case. Severe investigative practices on foreign territory could be considered an infringement of that country's sovereignty and therefore requires its permission or some sort of legal process, such as mutual legal assistance, which is not known for its efficiency. That still isn't enough to withstand what are Indian courtroom standards, however.

Such a measure as expanding the scope of Indian law in theory will not overcome the practical obstacles, the research indicates. Solid home rules on jurisdiction, fast and effective international cooperation, easy means to lock down electronic evidence, and strong protections for sovereignty and individual rights, are all necessary for real solutions.

As for the future, the regulation of cybercrime will not be a function of the way each country delineates its borders but more of a function of how willing each country is to cooperate with each other particularly when one crime can have ripple effects in a number of countries. International treaties such as the UN Convention against Cybercrime (which India signed September 2026 but has yet to come into force) could be useful. Ultimately, this will depend on the manner in which they are implemented in the countries and the extent to which the fundamental rights are kept in view.

REFERENCES

[1] Shillito, M. R. (2019). Untangling the 'Dark Web': An emerging technological challenge for the criminal law. Information & Communications Technology Law, 28(2), 186-207. doi.org. https://livrepository.liverpool.ac.uk/3041661/

[2] Ghappour, A. (2017). Searching places unknown: Law enforcement jurisdiction on the dark web. Stanford Law Review, 69, 1075-1136. ssrn.com https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2742706

[3] Arnell, P., & Faturoti, B. (2023). The prosecution of cybercrime: Why transnational and extraterritorial jurisdiction should be resisted. Informa UK Limited. worktribe.com https://rgu-repository.worktribe.com/output/1632111/the-prosecution-of-cybercrime-why-transnational-and-extraterritorial-jurisdiction-should-be-resisted

[4] de Hert, P., Parlar, C., & Sajfert, J. (2018). The Cybercrime Convention Committee's 2017 guidance note on production orders: Unilateralist transborder access to electronic evidence promoted via soft law. Computer Law & Security Review, 34(2), 323-336. doi.org https://research.tilburguniversity.edu/en/publications/the-cybercrime-convention-committees-2017-guidance-note-on-produc/

[5] Patra, S. (2025, March 19). Bharatiya Nyaya Sanhita, 2023 updates, comments, comparison with Indian Penal Code, 1860 part-1. Patra's Law Chambers. patraslawchambers.com https://patraslawchambers.com/?p=676

[6] Vidhi Judicial Academy. (2023). Section 113 of the Bharatiya Nagarik Suraksha Sanhita, 2023. vidhijudicial.com https://vidhijudicial.com/section-

113-of-the-bharatiya-nagarik-suraksha-sanhita,-2023.html

[7] European Union Agency for Law Enforcement Training. (2018). Darknet online module: Executive summary [Executive summary]. europa.eu https://www.cepol.europa.eu/sites/default/files/Executive Summary Darknet.pdf

[8] Journalism. University. (2026, February 10). The extra-territorial reach of India's IT Act: Jurisdiction in cyberspace. https://journalism.university/contemporary-scenario-of-digital-media/extra-territorial-reach-india-it-act/ https://journalism.university/contemporary-scenario-of-digital-media/extra-territorial-reach-india-it-act

[9] Kumar, A. (2017, March 3). Jurisdictional challenges while doing online transactions. iPleaders. https://blog.ipleaders.in/jurisdictional-challenges-while-doing-online-transactions/ https://blog.ipleaders.in/?p=21605

[10] bjo163. (2026, September). [AUTO-RESEARCH] LAW UN Convention against Cybercrime treaty-status applicability (Issue #127). GitHub. github.com https://github.com/bjo163/rocksoul-aws/issues/127

[11] Lawx.in. (2023). Section 63 of Bhartiya Sakshya Adhiniyam 2023. lawx.in https://lawx.in/acts/section/116/1033/8958

[12] Swire, P., Kennedy-Mayo, D., & Jayakumar, A. (2023, April 10). India's access to criminal evidence in the US: A proposed framework for an executive agreement (Issue Brief No. 631). Observer Research Foundation. orfonline.org https://www.orfonline.org/research/indias-access-to-criminal-evidence-in-the-us

[13] India's News.Net. (2026, October 4). EAM Jaishankar signs UN Convention against Cybercrime on UNGA sidelines. indiasnews.net http://www.indiasnews.net/news/279332450/eam-jaishankar-signs-un-convention-against-cybercrime-on-unga-sidelines