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

VOLUME 6 AND ISSUE 1 OF 2026

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

Published by

Institute of Legal Education

https://iledu.in

FROM TOR TO TRIAL: EVIDENTIARY CHALLENGES IN PROSECUTING DARK WEB CRIMES UNDER INDIAN CRIMINAL LAW

AUTHORS – SANSKRITI SHUKLA* & DR. SHAIWALINI SINGH**

* STUDENT AT AMITY UNIVERSITY UTTAR PRADESH LUCKNOW CAMPUS

** ASSISTANT PROFESSOR AT AMITY UNIVERSITY UTTAR PRADESH LUCKNOW CAMPUS

BEST CITATION – SANSKRITI SHUKLA & DR. SHAIWALINI SINGH, FROM TOR TO TRIAL: EVIDENTIARY CHALLENGES IN PROSECUTING DARK WEB CRIMES UNDER INDIAN CRIMINAL LAW, INDIAN JOURNAL OF LEGAL REVIEW (IJLR), 6 (1) OF 2026, PG. 973-983, APIS – 3920 – 0001 & ISSN - 2583-2344

Abstract

The Dark Web has grown at such a rapid pace that it has created new and unprecedented challenges for modern law enforcement agencies and criminal justice systems around the world. The Dark Web is characterized by its anonymity, encryption, and decentralized architecture and facilitates a wide range of criminal activities, such as drug trafficking, cyber fraud, terrorism financing, human trafficking, and the dissemination of illegal digital content. In the Indian scenario, although the existing cyber laws and criminal legislations attempt to regulate online delinquency, their ability to deal with crimes that originate from anonymized networks such as Tor is limited. Lawyers, investigators, and prosecutors face significant challenges in identifying the culprits, linking digital identities, and making electronic evidence admissible in courts.

This research paper critically analyzes the evidentiary complexities associated with the prosecution of crimes committed on the Dark Web in the context of Indian criminal law. It assesses the ability of the existing legal framework, specifically the Information Technology Act of 2000, the Indian Penal Code of 1860, and the Indian Evidence Act of 1872, to deal with encrypted digital evidence and international cyber crimes. It focuses on the procedural complexities, including the requirements of Section 65B of the Evidence Act, the chain of custody, jurisdictional conflicts, and the limitations of cyber forensic facilities.

In addition, the paper explores the conflict between law enforcement and the protection of constitutional rights, specifically the right to privacy and due process. By referring to judicial pronouncements, international best practices, and the latest technological developments, the paper suggests legal and institutional reforms to enhance the Indian cybercrime prosecution framework. It argues that a harmonious blend of technological development, procedural flexibility, and constitutional protection is required to ensure that the criminal justice system is effective and rights-respecting in countering the Dark Web threat.

Keywords

Dark Web, Tor Network, Indian Criminal Law, Digital Evidence, Cyber Forensics, Indian Evidence Act, Information Technology Act

1. Introduction

The internet has transformed the way we produce, access, and share information, connecting people and increasing efficiency like never before. However, it has also spawned invisible cyber worlds that we refer to as the

Dark Web[2167]. Access to it is through specialized software that ensures anonymity, most notably The Onion Router (Tor)[2168]. Unlike the surface web, the Dark Web is not searchable by conventional search engines and remains beyond the reach of conventional regulation. Users can conceal their identity and location, making it much more difficult to track them down. This anonymity has attracted a broad range of illicit activities, including drug and gun trafficking, child sexual abuse images, ransomware, identity theft, and sophisticated financial frauds, often transnational in nature.

The investigation of crimes that have their origin on the Dark Web is a very difficult task for law enforcement and the courts. A good case requires the collection, preservation, authentication, and admissibility of evidence in a manner that satisfies legal requirements. However, the nature of the Dark Web, with its end-to-end encryption[2169], routing, and hosting, makes it a very difficult environment to investigate. Trails are difficult to track down, linking a crime to a person is uncertain, and the authenticity of digital evidence is constantly in question.

In the Indian context, these challenges are further exacerbated by the framework of existing criminal and cyber laws[2170]. The courts struggle with the admissibility of electronic evidence, compliance with statutory requirements, and dealing with crimes that have transnational elements. In this context, this paper undertakes an in-depth analysis of the evidentiary and procedural challenges in prosecuting crimes that have their origin on the Dark Web under Indian criminal law and cyber law[2171], emphasizing the imperative need for legal and institutional adjustments.

2. Legal Framework Governing Cybercrimes in India

2.1 Indian Penal Code (IPC), 1860

The IPC contains provisions addressing cyber-related offences, such as:

- **Section 378/380/380** (Theft, House-Trespass, etc., including digital theft)
- **Section 420** (Cheating)
- **Section 463–465** (Forgery and its implications in digital forgery)

However, these sections were not originally designed for digital contexts and often require interpretative expansion.

2.2 Information Technology Act, 2000 (as amended)

The IT Act is the cornerstone of cyber legislation:

- **Section 66** and related provisions criminalise computer-related offences.
- **Section 65–66A (obsolete)** dealt with data misuse and obscenity.
- **Section 72A** penalises disclosure of sensitive personal data.
- **Section 78A–78D** empower seizure and retention of data.

Despite these provisions, digital evidence collected from encrypted Dark Web sources poses admissibility issues.

2.3 Indian Evidence Act, 1872

The Evidence Act was amended to accommodate digital evidence:

- **Section 65A & 65B** clarify admissibility of electronic records.

Section 65B(4) insists on certificate authentication for digital data, but in Dark Web cases, obtaining such certificates is often

[2167] Kaur, Shubhdeep, and Sukhchandan Randhawa. "Dark web: A web of crimes." Wireless Personal Communications 112.4 (2020): 2131-2158.
[2168] Dingledine, Roger, Nick Mathewson, and Paul Syverson. "Tor: The second-generation onion router." (2004).
[2169] Ermoshina, Ksenia, Francesca Musiani, and Harry Halpin. "End-to-end encrypted messaging protocols: An overview." International Conference on Internet Science. Cham: Springer International Publishing, 2016.
[2170] Ajayi, Emmanuel Femi Gbenga. "Challenges to enforcement of cyber-crimes laws and policy." Journal of Internet and Information Systems 6.1 (2016): 1-12.
[2171] Lodh, Shamik. "Unveiling the Dark Web: An Exploratory Study of AI-Assisted Cybercrime Investigations in India's Hidden Internet." LawFoyer Int'l J. Doctrinal Legal Rsch. 3 (2025): 129.

impracticable due to anonymity and lack of centralised servers.

3. Technical Complexities of the Dark Web

3.1 Encryption and Anonymity

One of the defining features of the Dark Web is its reliance on advanced encryption and privacy technology[2172], which differentiates it from the normal web. Consider Tor, for example, which uses a technique called routing, where your data is encrypted multiple times and routed through a series of randomly selected relay nodes before it reaches its final destination. Each node only knows the node that sent it the data and the node it sends it to, so there isn't a single point of knowledge that can identify the origin and destination of the message. This makes it difficult for users to be tracked, but it also makes it very difficult for law enforcement to track them down.

The problem for law enforcement is that it becomes difficult to identify the real-world location and identity of users who are engaging in criminal activity. Traditional methods of IP tracking[2173], geolocation, and server logs are not very effective because Tor is designed to prevent that kind of information from being gathered. This makes it difficult to assign jurisdiction, responsibility, and to connect the online activity to a real-world individual.

Following money on the Dark Web is also a complex process. Often, money is transferred using cryptocurrencies[2174], which, although having a public ledger, can be made difficult to track using money mixers or privacy-focused cryptocurrencies. This makes it difficult to connect the transaction, the digital wallet, and the individual.

The anonymity provided by encryption also makes it difficult to use digital evidence gathered during investigations. Screenshots, chat logs, or marketplace data may indicate that a crime has taken place, but they do not necessarily indicate who committed the crime. Without proper attribution, the usefulness of such evidence in court becomes questionable. Given the fact that Indian law requires proof beyond a reasonable doubt to establish criminal liability, such technology barriers seriously impede the prosecution of crimes, emphasizing the need for technology and legal adjustments to fill the anonymity gaps.

3.2 Volatile, Distributed Data

Another significant technical challenge posed by the Dark Web is that all the data exists in a constantly fluctuating, distributed manner. Unlike regular websites, which exist on fixed servers that are not likely to change, Dark Web markets and forums operate on a decentralized model that exists across multiple countries and regions. These sites are designed to be temporary in nature. Often, market sites suddenly go dark in what is known as "exit scams," where the site owners suddenly shut down and make off with the users' money, leaving little to no data that can be salvaged.

From an investigation standpoint, this makes it extremely difficult to quickly identify, collect, and preserve digital evidence. Data such as transaction records, messages, and user accounts can simply be erased once the servers are taken down or wiped clean. The data exists for such a short time that investigators are often forced to engage in real-time monitoring or undercover work, which requires significant resources and raises significant legal issues. Delays in securing search warrants, authorizations, or international assistance can mean that critical evidence is lost forever.

There is also the problem of preserving the integrity of the volatile Dark Web evidence without compromising the chain of custody. Evidence must be collected in a forensically sound manner to remain unchanged from the time of seizure to the time of presentation in

[2172] Sayyed, Hifajatali, and Sanu Rani Paul. "Exploring the role of encryption and the dark web in cyber terrorism: legal challenges and countermeasures in India." *Cogent Social Sciences* 11.1 (2025): 2479654.
[2173] Bujlow, Tomasz, et al. "A survey on web tracking: Mechanisms, implications, and defenses." Proceedings of the IEEE 105.8 (2017): 1476-1510.
[2174] Arıkan, Necip İhsan. "An Overview of the cryptocurrencies; the theory of money perspective." Malatya Turgut Özal Üniversitesi İşletme ve Yönetim Bilimleri Dergisi 1.2 (2020): 147-165.

court. In the case of Dark Web investigations, evidence is often collected through screenshots, mirror sites, or live recordings, which can be called into question for tampering and manipulation. The absence of original servers and metadata makes it even more difficult to authenticate.

In the Indian legal framework, it is essential to ensure that evidence meets specific standards for admissibility. If there is any compromise in the chain of custody or doubts about the integrity of the data, evidence may be deemed unreliable. Thus, the volatile and distributed nature of Dark Web data further exacerbates the difficulties of prosecution, underlining the need for specialized digital preservation techniques and legal guidelines to address these issues of evidentiary unreliability.

4. Evidentiary Challenges in Indian Context

4.1 Chain of Custody Issues

In criminal prosecutions, the chain of custody plays a crucial role in ensuring the admissibility and reliability of evidence. It refers to the chronological documentation that records the seizure, handling, transfer, storage, and analysis of evidence from the moment it is collected until it is produced before the court. Any gap or irregularity in this chain can raise doubts regarding the integrity of the evidence and may result in its exclusion. In cases involving Dark Web crimes, maintaining an unbroken chain of custody becomes particularly challenging due to the technical and transnational nature of digital evidence.

Dark Web investigations often involve data that is sourced from multiple digital devices, servers, and jurisdictions[2175]. Evidence may be collected through undercover operations, digital surveillance, foreign law enforcement agencies, or international service providers. Each transfer of data increases the risk of inadvertent alteration or procedural non-compliance. Moreover, the absence of physical evidence and reliance on electronic records heightens judicial scrutiny regarding authenticity and tampering.

In the Indian context, courts have consistently emphasised strict adherence to evidentiary procedures, especially in relation to electronic evidence. Investigators are required to demonstrate that digital data has not been manipulated at any stage. However, when evidence originates from anonymised networks and foreign servers, documenting every stage of handling becomes complex. Delays in mutual legal assistance, differing forensic standards, and jurisdictional overlaps further complicate this process.

As a result, even when substantive proof of criminal activity exists, prosecutions may falter due to procedural lapses in establishing a clear chain of custody. This highlights the need for standardised cyber forensic protocols and enhanced international cooperation to ensure the evidentiary integrity of Dark Web-related prosecutions under Indian criminal law.

4.2 Authentication of Digital Evidence

Per Section 65B, electronic evidence must be proven through a certificate specifying how data was stored and retrieved. With data from anonymised networks:

- Certificate generation may be impossible
- Forensic labs may lack tools to establish authenticity

Indian courts have sometimes rejected electronic data for want of proper certification. This statutory requirement, though intended to ensure reliability, poses serious practical difficulties in cases involving Dark Web crimes.

Data sourced from anonymised networks such as Tor is often extracted from concealed servers, encrypted platforms, or ephemeral marketplaces that lack identifiable administrators or traceable system owners. In such circumstances, the generation of a Section 65B certificate becomes virtually impossible, as

[2175] Ghappour, Ahmed. "Searching places unknown: Law enforcement jurisdiction on the dark web." Stan. L. Rev. 69 (2017): 1075.

INDIAN JOURNAL OF LEGAL REVIEW [IJLR – IF SCORE – 7.58]
VOLUME 6 AND ISSUE 1 OF 2026
APIS – 3920 - 0001 *(and)* ISSN - 2583-2344
Published by
Institute of Legal Education
https://iledu.in

there is no legally recognisable person who can certify the functioning or ownership of the device or network from which the data originated. Consequently, investigators are compelled to rely on secondary evidence such as screenshots, mirror images, or intercepted communications, the authenticity of which is frequently contested by the defence.

Furthermore, many forensic laboratories in India face infrastructural and technical limitations in verifying the authenticity of encrypted and anonymised digital artefacts. The absence of advanced decryption tools, standardised forensic methodologies, and trained personnel often undermines the evidentiary value of the data collected. Indian courts, adhering strictly to statutory mandates and judicial precedents, have on several occasions rejected electronic evidence due to non-compliance with certification requirements. This judicial approach, while legally sound, has inadvertently resulted in the weakening of prosecutions involving complex cybercrimes.

In the context of Dark Web offences, this evidentiary rigidity exposes a critical gap between technological realities and legal procedures. Unless alternative methods of authentication are judicially recognised or legislatively incorporated, the prosecution of such crimes is likely to remain fraught with evidentiary uncertainty

4.3 Jurisdictional Challenges

Many Dark Web crimes involve servers or actors overseas, raising:

- Extradition questions
- Mutual Legal Assistance Treaty (MLAT) delays[2176]

Delays in obtaining foreign cooperation impact evidence preservation. Jurisdictional issues constitute another major evidentiary and procedural hurdle in the prosecution of Dark Web crimes. Owing to the borderless nature of the internet and the decentralised architecture of Dark Web platforms, criminal activities often involve servers located in foreign jurisdictions and actors operating across multiple countries. This transnational dimension complicates the assertion of territorial jurisdiction under Indian criminal law and raises complex questions relating to extradition and international cooperation.

In many cases, the identification and apprehension of accused persons require extradition from foreign states, a process governed by bilateral treaties and diplomatic negotiations. Such procedures are often time-consuming and subject to political and legal constraints, thereby delaying the course of investigation and trial. Similarly, access to crucial digital evidence stored on overseas servers depends upon Mutual Legal Assistance Treaties (MLATs). Requests made under MLAT frameworks frequently suffer from prolonged delays due to bureaucratic formalities and differing legal standards across jurisdictions.

These delays have a direct and adverse impact on evidence preservation. Digital data on Dark Web platforms is highly volatile and may be deleted, altered, or rendered inaccessible before legal assistance is granted. Consequently, investigators may lose access to vital evidence necessary to establish guilt. The cumulative effect of these jurisdictional constraints significantly weakens prosecutorial efforts, underscoring the need for streamlined international cooperation mechanisms and faster legal processes to effectively address transnational Dark Web offences.

4.4 Encryption and Decryption

Encryption serves as a cornerstone of security and privacy on the Dark Web, but it simultaneously operates as a significant impediment to criminal investigations. Dark Web communications and data storage are typically protected through strong cryptographic techniques, including end-to-end encryption, which ensures that only the intended sender and recipient possess the keys

[2176] Swire, Peter, and Justin D. Hemmings. "Re-engineering the mutual legal assistance treaty process." *online], http://www. heinz. cmu. edu/~ acquiti/SHB2015/Swire. docx* (2015).

necessary to decrypt the information. In most cases, these private encryption keys are exclusively held by offenders, rendering the data inaccessible to law enforcement agencies without their voluntary cooperation.

The inability to decrypt seized devices or intercepted communications severely restricts investigative progress. Even when devices are lawfully confiscated, encrypted data may remain unreadable, preventing authorities from uncovering incriminating communications, transaction histories, or operational networks. Law enforcement agencies are often compelled to rely on sophisticated decryption tools or techniques, such as brute-force attacks or forensic exploits. However, such tools are either technologically inadequate, prohibitively expensive, or unavailable to investigative agencies in India due to infrastructural limitations.

Moreover, the use of intrusive decryption methods raises serious legal and constitutional concerns. Without proper judicial authorisation, attempts to bypass encryption safeguards may violate procedural due process and the right to privacy. Courts are increasingly vigilant in scrutinising the legality of such investigative techniques, particularly in light of constitutional protections against unreasonable search and seizure. As a result, investigators find themselves constrained between technological barriers and legal safeguards.

This dilemma underscores the pressing need for a coherent legal framework that enables lawful access to encrypted data under strict judicial oversight, while simultaneously safeguarding individual rights. Without such clarity, encryption will continue to pose a formidable obstacle in prosecuting Dark Web-related offences.

5. Case Law Survey

- **State of Tamil Nadu v. Suhas Katti (2004)**[2177]: The first conviction in India under the IT Act, Section 67, for sending obscene messages about a victim in online chat rooms. It was an indication that the IT Act can be used together with the IPC (now BNS) to combat online harassment.

- **Shreya Singhal v. Union of India (2015)**[2178]**:** Nullified Section 66A of the IT Act, which was being used to suppress online freedom of speech. It reinforced that the constitutional guarantee of freedom of speech in Article 19 applies to the online world as well.

- **Justice K.S. Puttaswamy v. Union of India (2017)**[2179]**:** Reaffirmed privacy as a constitutional right, which has implications for law enforcement agencies on surveillance, decryption of data, and the seizure of digital devices.

- **Ritu Kohli Case (2001)**[2180]**:** One of the earliest cases of cyber stalking and identity theft, in which the Delhi Cyber Cell used Section 66C of the IT Act for digital impersonation.

5.2 International Precedents

In **Volodina v. Russia** (No. 2), 2021, the court held that Russia failed to protect a woman who was a victim of cyberviolence from her ex-partner, for example, non-consensual sharing of intimate images and GPS tracking. The lack of action from the police constituted a violation of Article 8, which safeguards private life.

Buturugă v. Romania, 2021, represented a turning point in the court's decisions, as the court held that accessing a partner's private Facebook messages and files constitutes an infringement of privacy and domestic violence, which needs an effective investigation.

In Khadija Ismayilova v. Azerbaijan, 2019[2181], the court highlighted the state's failure to investigate sextortion and the dissemination of private videos involving a well-known journalist,

[2177] Sharma, Nikita, and Sakshi Vadhera. "Case Commentary: State of Tamil Nadu vs Suhas Katti." Available at SSRN 3776961 (2021).

[2178] Bhadauria, Anshika. "Shreya Singhal v/s Union of India (2013) 12 SCC 73." Supremo Amicus 9 (2019): 55.

[2179] GN, Pooja. "Justice KS Puttaswamy (RETD) VS. Union of India & ORS." Union of India & ORS (march 31, 2023) (2023).

[2180] THAKUR, DR SHWETA. "Cyber Crimes and Victimisation of Women in India with Special Reference to Cyber Obscenity."

[2181] Geybulla, Arzu. "Uncensored journalism in censored times: Challenges of reporting on Azerbaijan." Journalism 24.2 (2023): 313-327.

connecting the cybercrime to her journalistic activities.

6. Comparative Analysis: International Best Practices

6.1 United States

The United States has developed a comparatively advanced and adaptive legal framework to address cybercrimes, including those originating from the Dark Web. A combination of substantive criminal statutes, procedural tools, and institutional expertise enables U.S. law enforcement agencies to investigate and prosecute complex digital offences more effectively. Key legislations such as the Computer Fraud and Abuse Act (CFAA) and the Racketeer Influenced and Corrupt Organizations Act (RICO) provide broad jurisdictional reach and flexibility to address organised cybercriminal activity, including online marketplaces operating on anonymised networks.

The U.S. legal system places significant emphasis on electronic surveillance and undercover operations, subject to judicial oversight. Law enforcement agencies routinely employ controlled buys, network infiltration, and advanced cyber forensic techniques to gather admissible evidence from Dark Web platforms. Additionally, U.S. courts have demonstrated a pragmatic approach toward the admissibility of digital evidence, focusing on reliability and probative value rather than rigid formalism. Federal agencies such as the FBI and DEA are equipped with specialised cybercrime units and cutting-edge forensic infrastructure capable of decrypting data, analysing blockchain transactions, and linking digital identities to real-world actors.

Moreover, strong inter-agency coordination and expedited international cooperation mechanisms enable timely access to cross-border evidence. The U.S. approach illustrates how legislative flexibility, technological capacity, and judicial pragmatism can collectively enhance the effectiveness of prosecuting Dark Web crimes, offering valuable lessons for the Indian criminal justice system.

6.2 European Union

The European Union has adopted a harmonised and rights-centric approach to combating cybercrime, balancing effective law enforcement with robust data protection standards. Through instruments such as the EU Framework Decision on Attacks against Information Systems, member states are encouraged to criminalise a wide spectrum of cyber offences and align their investigative and evidentiary practices. This harmonisation facilitates cross-border cooperation, which is crucial in addressing Dark Web crimes that transcend national boundaries.

A defining feature of the EU approach is the emphasis on standardised cyber evidence protocols. Member states are required to ensure the proper collection, preservation, and exchange of electronic evidence in a manner that maintains integrity and authenticity. Institutions such as Europol and Eurojust play a pivotal role in coordinating investigations, sharing intelligence, and assisting national authorities in complex cybercrime prosecutions. These bodies provide technical expertise and facilitate joint investigation teams, reducing procedural delays.

Simultaneously, the General Data Protection Regulation (GDPR) imposes strict safeguards on data processing, ensuring that investigative measures respect privacy and proportionality. While this may constrain unchecked surveillance, it reinforces public trust and constitutional legitimacy. The EU model demonstrates that effective prosecution of Dark Web crimes need not come at the cost of fundamental rights, offering a balanced framework that India may draw upon while reforming its cybercrime enforcement mechanisms.

INDIAN JOURNAL OF LEGAL REVIEW [IJLR – IF SCORE – 7.58]
VOLUME 6 AND ISSUE 1 OF 2026
APIS – 3920 - 0001 *(and)* ISSN - 2583-2344
Published by
Institute of Legal Education
https://iledu.in

7. Proposed Reforms for Indian Legal System

7.1 Amendments to Evidence Act

One of the most pressing reforms required in the Indian legal framework is the modernization of the Indian Evidence Act, 1872 to address the practical difficulties associated with electronic evidence in Dark Web prosecutions. The rigid requirement of Section 65B certification, though designed to ensure authenticity, often becomes impracticable in cases involving anonymised networks, encrypted platforms, and foreign servers. In such scenarios, strict insistence on certification may defeat the ends of justice by excluding otherwise reliable evidence.

To address this gap, the law should recognise acceptable alternatives to Section 65B certification where compliance is impossible despite due diligence. Courts may be empowered to rely on expert-verified forensic logs, hash value authentication, and blockchain-backed timestamps to establish data integrity. Judicial discretion may also be expanded to admit electronic evidence based on credibility, reliability, and corroboration rather than formal certification alone. Such amendments would align evidentiary standards with technological realities while preserving safeguards against manipulation. A flexible yet principled approach would significantly strengthen prosecutorial capacity in complex cybercrime cases without undermining procedural fairness.

7.2 Specialized Cyber Courts

The establishment of specialised cyber courts represents a crucial institutional reform for effectively adjudicating Dark Web-related offences. Conventional criminal courts often lack the technical expertise required to evaluate complex digital evidence involving encryption, blockchain transactions, and cyber forensic methodologies. This knowledge gap can result in misinterpretation of evidence, procedural delays, and inconsistent judicial outcomes.

Specialised cyber courts equipped with technically trained judges or assisted by court-appointed cyber experts would enhance judicial competence in handling such matters. These courts could adopt streamlined procedures for the admission and evaluation of electronic evidence, reducing delays caused by prolonged expert testimony. Additionally, specialised courts would promote uniformity in judicial interpretation of cyber laws and evidentiary standards. By fostering judicial specialisation, India can ensure faster, more accurate, and technologically informed adjudication of cybercrime cases while maintaining due process guarantees.

7.3 Mutual Legal Assistance Modernisation

Given the transnational nature of Dark Web crimes, modernising India's Mutual Legal Assistance mechanisms is essential for effective investigation and prosecution. Current MLAT procedures are often criticised for being slow, bureaucratic, and ill-suited to the volatile nature of digital evidence. Delays in obtaining foreign assistance frequently result in the loss or destruction of crucial data.

Reforms should focus on introducing expedited digital request systems, predefined timelines for compliance, and automatic evidence-sharing mechanisms with trusted jurisdictions. Bilateral and multilateral agreements may incorporate standardised cyber evidence protocols to facilitate swift cooperation. Strengthening coordination between investigative agencies and diplomatic channels would further enhance efficiency. Modernised MLAT frameworks would significantly improve evidence preservation and attribution in Dark Web cases, ensuring that jurisdictional barriers do not undermine justice.

7.4 Improved Forensic Infrastructure

Robust forensic infrastructure is the backbone of effective cybercrime prosecution. In India, investigative agencies and forensic laboratories often face limitations in terms of advanced tools, technical expertise, and specialised training required to deal with Dark Web technologies. This inadequacy hampers efforts

to decrypt data, analyse encrypted traffic, and attribute digital conduct to specific individuals.

Substantial investment is required in developing state-of-the-art cyber forensic laboratories equipped with advanced decryption tools, blockchain analytics software[2182], and traffic analysis capabilities. Continuous training programmes should be instituted to equip investigators, prosecutors, and forensic experts with evolving technological skills. Collaboration with academic institutions and private cybersecurity firms may further enhance technical capacity. Strengthening forensic infrastructure would not only improve evidentiary reliability but also increase conviction rates, thereby reinforcing the credibility and effectiveness of India's cybercrime enforcement framework.

8. Balancing Civil Liberties and Surveillance

The increasing reliance on surveillance and lawful interception as tools to combat Dark Web–related crimes presents a profound constitutional dilemma for modern democracies. While the anonymity and encryption inherent to the Dark Web necessitate enhanced investigative powers, any expansion of state surveillance must operate within the confines of constitutional safeguards. In India, this balance is particularly delicate, as the criminal justice system must reconcile effective law enforcement with the protection of individual liberties guaranteed under the Constitution.

The recognition of the **right to privacy as a fundamental right** in *Puttaswamy v. Union of India* has significantly reshaped the legal discourse surrounding surveillance. The Supreme Court held that any infringement of privacy must satisfy the tests of legality, necessity, proportionality, and procedural safeguards. In the context of Dark Web investigations, this implies that indiscriminate or mass surveillance, even if technologically feasible, would be constitutionally impermissible. Lawful interception must therefore be narrowly tailored, based on reasonable suspicion, and authorised through transparent legal processes.

Procedural safeguards against unreasonable search and seizure assume heightened importance in cyber investigations. Unlike physical searches, digital surveillance can be covert, continuous, and deeply intrusive, often capturing vast amounts of personal data unrelated to the alleged offence. Without adequate checks, such powers risk misuse, chilling effects on free expression, and erosion of public trust in state institutions. Judicial oversight, time-bound authorisations, accountability mechanisms, and post-surveillance review processes are essential to prevent abuse.

At the same time, an overly restrictive approach may render law enforcement agencies ineffective against sophisticated cybercriminal networks operating beyond national borders. Therefore, reforms aimed at enhancing surveillance capabilities must be accompanied by strong institutional safeguards, clear statutory limits, and effective remedies for rights violations. A constitutionally compliant framework that harmonises civil liberties with enforcement imperatives is crucial. Only by maintaining this balance can India ensure that its response to Dark Web crimes remains both effective and faithful to the rule of law.

9. Conclusion

The Dark Web has brought a paradigm shift in cybercrime, making it difficult for conventional law enforcement agencies to act. The Dark Web's reliance on anonymity, encryption, and peer-to-peer networks has created a challenge for existing laws and procedures. In India, despite the development of new cyber laws and judicial interpretations, criminal cases that originate from hidden cyber networks are difficult to manage. Challenges such as identifying who committed an act, authenticating electronic records, maintaining

[2182] Xu, Xiwei, et al. "The blockchain as a software connector." 2016 13th Working IEEE/IFIP Conference on Software Architecture (WICSA). Ieee, 2016.

a clear chain of custody, and handling cross-border crimes remain a challenge to successful prosecution.

This paper illustrates that most of these challenges arise from the mismatch between rapidly evolving technology and rigid, unchanging laws. Existing laws on electronic evidence are inadequate when dealing with the Dark Web's anonymous and encrypted networks. Thus, prosecutions remain unsuccessful not because crimes did not occur, but because of the mismatch between procedures and evidence. This is detrimental to deterrence, trust in cybercrime enforcement, and leaves clever criminals exploiting loopholes in the law.

Addressing these challenges requires a comprehensive overhaul of the system. Laws must incorporate dynamic procedures without undermining the integrity of evidence. Simultaneously, there must be substantial investment in cyber forensics and training to enable investigators to address technological challenges. Since Dark Web crimes are cross-border, improved international cooperation and facilitation of mutual legal assistance are also necessary.

Any proposed overhaul must remain consistent with constitutional values. An expansion of investigative powers must not impinge upon rights such as privacy, due process, and liberty. A rights-based and rights-balanced framework is necessary to ensure effective enforcement and constitutional protection. Only a thoughtful and value-driven approach can enable Indian criminal law to effectively address the challenges posed by the Dark Web.

References

1. Indian Penal Code, 1860.
2. Information Technology Act, 2000.
3. Indian Evidence Act, 1872.
4. Puttaswamy v. Union of India (Privacy Judgment).
5. Lodh, Shamik. "Unveiling the Dark Web: An Exploratory Study of AI-Assisted Cybercrime Investigations in India's Hidden Internet." LawFoyer Int'l J. Doctrinal Legal Rsch. 3 (2025): 129.
6. Sayyed, Hifajatali, and Sanu Rani Paul. "Exploring the role of encryption and the dark web in cyber terrorism: legal challenges and countermeasures in India." Cogent Social Sciences 11.1 (2025): 2479654.
7. Bujlow, Tomasz, et al. "A survey on web tracking: Mechanisms, implications, and defenses." Proceedings of the IEEE 105.8 (2017): 1476-1510.
8. Arıkan, Necip İhsan. "An Overview of the cryptocurrencies; the theory of money perspective." Malatya Turgut Özal Üniversitesi İşletme ve Yönetim Bilimleri Dergisi 1.2 (2020): 147-165.
9. Ghappour, Ahmed. "Searching places unknown: Law enforcement jurisdiction on the dark web." Stan. L. Rev. 69 (2017): 1075.
10. Swire, Peter, and Justin D. Hemmings. "Re-engineering the mutual legal assistance treaty process." online], http://www. heinz. cmu. edu/~ acquiti/SHB2015/Swire. docx (2015).
11. Sharma, Nikita, and Sakshi Vadhera. "Case Commentary: State of Tamil Nadu vs Suhas Katti." Available at SSRN 3776961 (2021).
12. Bhadauria, Anshika. "Shreya Singhal v/s Union of India (2013) 12 SCC 73." Supremo Amicus 9 (2019): 55.
13. GN, Pooja. "Justice KS Puttaswamy (RETD) VS. Union of India & ORS." Union of India & ORS (march 31, 2023) (2023).
14. THAKUR, DR SHWETA. "Cyber Crimes and Victimisation of Women in India with Special Reference to Cyber Obscenity."

15. Geybulla, Arzu. "Uncensored journalism in censored times: Challenges of reporting on Azerbaijan." Journalism 24.2 (2023): 313-327.

16. Xu, Xiwei, et al. "The blockchain as a software connector." 2016 13th Working IEEE/IFIP Conference on Software Architecture (WICSA). Ieee, 2016.