TPM Vol. 32, No. S7, 2025
ISSN: 1972-6325
https://www.tpmap.org/

Open Access

LEGAL & PSYCHOLOGICAL DIMENSIONS OF DARK WEB EXPOSURE AND YOUTH VICTIMIZATION: EVIDENTIARY CHALLENGES UNDER THE BHARATIYA SAKSHYA ADHINIYAM

SHALU MEHTA
RESEARCH SCHOLAR, DEPARTMENT OF LAW, SURESH GYAN VIHAR UNIVERSITY, JAIPUR (RAJASTHAN),
EMAIL ID- shaluyadav593@gmail.com

PROF.(DR.) VENOO RAJPUROHIT
HEAD OF DEPARTMENT, DEPARTMENT OF LAW, SURESH GYAN VIHAR UNIVERSITY, JAIPUR RAJASTHAN,
EMAIL ID venoo.rajpurohit@mygyanvihar.com

ABSTRACT
The rise of the dark web has significantly altered digital crime landscapes across the globe, including India. Responding to evolving technological realities, the Bharatiya Sakshya Adhiniyam, 2023 (BSA) replaces the Indian Evidence Act, 1872, with replacement updating the evidentiary norms for electronic records, digital forensics, and cyber-crime investigations. This research paper examines the legal and psychological dimensions of dark web exposure, particularly among youth aged 18years to 45years, including men, women, and transgender individuals. While the dark web enables anonymity, encrypted transactions, and unregulated content exchange, it has simultaneously facilitated illegal drug marketplaces, cyber-exploitation, data trafficking, red-room myths, terrorist propaganda, and pornography trade. Law enforcement faces critical evidentiary challenges in retrieving, authenticating, and presenting dark web–based data in Indian courts under the new act. Alongside legal complexities, prolonged or accidental exposure to dark web content induces fear conditioning, desensitisation to violence, disinhibition, anxiety, growth of deviant fantasies, addiction, and moral numbness in young adults. This paper integrates legal frameworks with behavioural science to highlight the need for psycho-legal interventions, awareness programmes, capacity-building for digital forensics, and judicial readiness for cyber-evidence. The research uses secondary sources to analyse statutes, articles, psychological reports, and case-based interpretations.
Keywords Dark web, Victimization, Bharatiya Sakshya Adhiniyam, digital evidence, witness testimony, eyewitness reliability, memory distortion, psychological factors, forensic evidence, fair trial

INTRODUCTION

The rapid evolution of digital communication, cyber interaction, and technologically-mediated social behaviour has deeply influenced both the legal framework and psychological well-being of individuals in the contemporary era. With the enforcement of the Bharatiya Sakshya Adhiniyam (BSA), 2023- India's reformed evidentiary law replacing the Indian Evidence Act, 1872- a new paradigm has emerged that redefines the principles of admissibility, credibility, and proof of digital evidence. The Act recognises the expanding domain of cyber-generated information, electronically stored content, and digitally induced vulnerabilities, thereby creating a structural foundation to address crimes arising from online exposure, exploitation, and victimisation. However, while the law introduces progressive mechanisms for handling electronic records, it simultaneously raises complex questions about consent, mental harm, privacy infringement, and the psychological trauma experienced by individuals involved in such cases. Understanding the convergence of legal procedures and human behavioural responses therefore becomes essential in evaluating the real-world application of the Act.

Exposure in the digital environment- whether intentional or coerced- can have profound psychological implications. Victims subjected to online harassment, stalking, cyberbullying, sexual exploitation, or defamation often experience anxiety, shame, social withdrawal, and long-term trauma. These emotional responses impact their capacity to narrate incidents clearly, recall details consistently, or participate confidently in trial proceedings. The Bharatiya Sakshya Adhiniyam underscores the importance of testimony reliability, but the psychological state of a witness or victim can influence memory retention, perception of events, and responsiveness during cross-examination. Thus, the law must not only focus on the technical authenticity of evidence but also remain sensitive to the mental state of individuals

whose experiences form the basis of proof. In cases of minors or persons under emotional distress, additional safeguards become indispensable to ensure fairness, accuracy, and minimisation of re-traumatisation.

Evidentiary challenges represent a core concern within the BSA framework, particularly in matters involving digital traces. Issues such as data manipulation, metadata alteration, anonymisation, deepfake generation, and jurisdictional ambiguity complicate the establishment of authenticity and chain of custody. The Act attempts to modernise admissibility standards through recognition of electronic documents, server logs, digital footprints, and secondary evidence, but the burden of proving integrity and originality remains steep. Psychological pressure further intensifies when victims are required to relive traumatic experiences while defending their credibility against technological loopholes exploited by perpetrators. Moreover, social stigma or fear of retaliation may inhibit reporting, thereby weakening evidentiary continuity and depriving the legal system of vital testimony.

The intersection between law and psychology under the Bharatiya Sakshya Adhiniyam therefore calls for a holistic interpretative approach. Legal reforms must be supplemented by trauma-informed investigation methods, sensitive witness examination procedures, digital forensic competence, and protective mechanisms for vulnerable individuals. The true potential of the Act lies not only in its statutory language but in its ability to balance evidentiary rigour with human dignity. Acknowledging the psychological complexities of exposure is imperative for ensuring justice, while strengthening evidentiary standards is crucial for maintaining judicial integrity. Together, these dimensions shape a transformative pathway for fair, empathetic, and technologically resilient justice administration in India.

The present paper merges psychological effects and legal challenges, highlighting how the Bharatiya Sakshya Adhiniyam deals with modern evidence and what improvements may strengthen India's cyber-justice system.

RESEARCH QUESTIONS

1. What psychological impact does dark web exposure create among youth aged from 18 years to 45 years and how do prolonged interactions affect mental health and behavioural outcomes?
2. How effectively does the Bharatiya Sakshya Adhiniyam, 2023 address evidentiary challenges related to digital and dark web-based crimes in India?
3. What improvements are required in investigation, digital forensics, and judicial interpretation for reliable admission of darknet evidence in Indian courts?

METHODOLOGY (SECONDARY RESEARCH)

This study employs a secondary research approach, drawing on legal texts, judicial precedents, psychological literature and existing empirical data to examine dark-web-related youth victimization under the Bharatiya Sakshya Adhiniyam (BSA). A doctrinal review of the BSA and reported cases will identify key evidentiary challenges, particularly regarding digital anonymity and forensic reliability. Psychological studies on online harm, grooming, and child testimony will contextualize victim experiences.

Relevant statistical reports and cybercrime datasets will be synthesized to assess trends in digital evidence use and case outcomes. Together, these sources provide a consolidated basis for evaluating the adequacy of the BSA in addressing dark-web-facilitated offenses against youth.

LITERATURE REVIEW

Existing psychological literature notes that exposure to violent or explicit online content alters neural response patterns in young adults. Researchers highlight **desensitisation theory**, where emotional response weakens as one repeatedly observes disturbing scenes. Dark web forums host uncensored violent media, trafficking networks, and drug markets, making youth particularly vulnerable to emotional numbing and thrill reinforcement. Scholars observe that anonymity emboldens curiosity and risk-taking, drawing individuals deeper into exploitation rings.

A second stream of research concentrates on cyber-addiction and compulsive behaviour. Studies show that darknet platforms amplify behavioural reinforcement, especially among technologically skilled youth. The interface itself creates a sense of secrecy and power, which escalates nighttime browsing, porn consumption, hacking participation, or cryptocurrency-based gambling. Researchers argue that this category of exposure is highly habit-forming, often correlated with depression, sleep-cycle disruption, and declining empathy.

Regarding legal scholarship, authors critique the inadequacy of the older Indian Evidence Act in dealing with encrypted evidence and blockchain transactions. Research highlights gaps in proving authorship, authenticity, and integrity of digital records. The Bharatiya Sakshya Adhiniyam addresses admissibility of electronic documents, provides expanded definitions, and recognises metadata, digital signatures, and hash verification — yet scholars agree that the technical capacity of investigators remains insufficient.

Finally, forensic literature repeatedly stresses the difficulty of traceability within dark web crimes. International comparative studies show that seamless evidence collection requires advanced cyber-forensics, mirror server imaging,

ISP-level interception, and judicial cooperation across jurisdictions. While the BSA provides the legal foundation, implementation remains limited without skilled manpower and continuous technological training.

UNDERSTANDING THE DARK WEB: STRUCTURE & RISK

The dark web represents a concealed layer of the internet, accessible only through anonymizing tools like Tor, I2P, or Freenet. Unlike the surface web indexed by search engines or the deep web consisting of databases and private networks, the dark web operates on encrypted pathways that obscure user identity and location. Its architecture comprises hidden services identifiable through .onion addresses, decentralized hosting, peer-to-peer routing, and multiple layered encryption protocols. These features make surveillance and traceability complex, creating an ecosystem where illicit exchanges- drug trafficking, child abuse material, organ trade, ransomware markets, cryptocurrency laundering, and extremist networks- flourish outside traditional legal oversight. However, the same architecture also supports political dissidents, whistleblowers, and journalists seeking anonymity in oppressive environments, making the dark web a dual-use technological space.

Exposure to dark web environments poses multi-layered risks. Legally, users may unwittingly encounter criminal content, engage in transactions that violate cybercrime laws, or leave digital footprints leading to liability under the Information Technology Act, 2000, and related penal statutes. For investigators, attribution becomes difficult because servers are globally distributed, identities masked through VPNs, multi-hop relays, cryptocurrency tumblers, and encrypted messaging. The Bharatiya Sakshya Adhiniyam, replacing the Indian Evidence Act in 2023, demands specific standards for the admissibility, integrity, and authentication of electronic evidence. Proving the origin, authorship, and chain of custody of dark web material therefore presents inherent evidentiary challenges. Screenshots or intercepted pages cannot suffice on their own unless corroborated by metadata, hash values, digital signatures, server seizure records, or testimony validating forensic extraction. Because dark web nodes frequently disappear or relocate, establishing continuity of evidence, maintaining tamper-proof logs, and demonstrating the reliability of forensic tools becomes critical for prosecution.

Psychologically, dark web exposure can be deeply damaging, especially for minors and vulnerable individuals. Repeated interaction with violent content, exploitation videos, or extremist propaganda can desensitize emotions, normalize deviance, and escalate curiosity toward criminal behavior. Youth may be manipulated into sharing personal information, coerced into illegal acts, or lured into self-harm communities. The anonymity that empowers free speech also emboldens predators, leading to grooming, identity theft, cyberbullying, sextortion, and mental distress. Victims often experience shame, fear of disclosure, and long-term trauma, reducing their willingness to report incidents, which further complicates the evidentiary chain. Courts under the Bharatiya Sakshya Adhiniyam 2023 require victim statements to be precise, reliable, and corroborated with digital traces, but psychological distress may impact memory recall, consent understanding, and testimonial strength.

Therefore, understanding the structure of the dark web is essential not only for cyber-forensics and legal practitioners but also for psychologists, educators, and policy-makers. Strong digital literacy, parental guidance, surveillance monitoring, and anonymous reporting frameworks are crucial to mitigating harm. On the legal front, capacity-building for investigation agencies, specialized cyber-forensic units, cross-border cooperation, and standardized protocols for seizure and authentication of electronic evidence become imperative. Ultimately, balancing privacy rights with security, and technological anonymity with accountability, forms the core of contemporary challenges under the Bharatiya Sakshya Adhiniyam 2023 when confronting the evolving risks of the dark web.

PSYCHOLOGICAL IMPACT ON YOUTH

The increasing exposure of young individuals to unsafe online environments, violent content, digital exploitation, and dark-web related activities has generated complex legal and psychological implications. While the Bharatiya Sakshya Adhiniyam, 2023 provides a modern framework for evidence collection, digital proof validation, and admissibility in cyber-related offences, understanding the psychological impact on youth remains equally crucial. Exposure to illicit online interactions can alter emotional regulation, perception of safety, identity formation, and long-term behavioural patterns. Thus, any discourse on evidentiary standards must be accompanied by an understanding of psychological vulnerabilities faced by children and adolescents who become victims or witnesses in such matters.

One of the most pressing psychological consequences is trauma resulting from exposure to sexual exploitation, cyberbullying, grooming, or violent imagery. Young minds operate in a stage of neural development where emotional control and decision-making systems are still evolving. Traumatic online encounters can trigger anxiety, depression, PTSD-like symptoms, sleep disorders, and academic disengagement. Victims may struggle to articulate experiences during legal proceedings, particularly under cross-examination, where reliving the incident often re-induces emotional distress. The Bharatiya Sakshya Adhiniyam, while permitting electronic and digital evidence to reduce testimonial burden, still requires victim statements, making trauma-informed judicial procedures necessary.

Digital victimisation also affects identity and self-worth. Adolescents place high value on peer approval and social perception. Cyber exploitation, defamation, or privacy breaches may lead to shame, withdrawal, or aggressive retaliation. When their personal images or conversations are circulated online, the fear of lifelong digital permanence amplifies psychological pain. The evidentiary process can also heighten this distress, as devices, chat logs, or media

files become part of the courtroom record. Without sensitive handling, evidentiary scrutiny may feel like public exposure rather than protection.

Additionally, repeated exposure to dark-web content- such as drug markets, weapon trade, violent pornography, or extremist forums- can desensitise young users. This may normalize deviant behaviour, distort moral judgment, and increase risk-taking tendencies. Legal systems face challenges in distinguishing between intentional participation and manipulated involvement, especially where minors are coerced or psychologically conditioned. The Bharatiya Sakshya Adhiniyam emphasis on the authenticity and integrity of digital evidence is relevant here, as encrypted or anonymous platforms often erase traces of coercion, making psychological assessment key in attributing culpability.

Another dimension is testimonial competency. Many young victims fear retaliation from perpetrators or social stigma, leading to reluctance in reporting. During evidence collection, fragmented memory, emotional shutdown, or inconsistent narration may be misconstrued as unreliability. Courts, therefore, must integrate child-sensitive deposition procedures, closed-court testimonies, expert psychological evaluation, and digital evidence support to reduce dependency on verbal recall. The interplay of clinical findings with digital proof enhances evidentiary credibility while safeguarding mental well-being.

The psychological impact on youth in digital exploitation cases cannot be separated from legal evidentiary challenges. The Bharatiya Sakshya Adhiniyam provides a robust digital evidence framework, but its application must be complemented by trauma-informed investigation, sensitive witness handling, and psychological assessment. Only through integration of legal precision and psychological insight can justice be delivered without re-victimisation, ensuring that young individuals emerge not only legally protected but emotionally restored.

LEGAL DIMENSIONS UNDER THE BHARATIYA SAKSHYA ADHINIYAM (2023)

The Bharatiya Sakshya Adhiniyam, 2023 (BSA) fundamentally reshapes the legal framework of evidence in India and has direct implications for understanding the legal and psychological dimensions of exposure, especially in technology-driven offences and digital victimisation. Replacing the Indian Evidence Act, 1872, the BSA re-codifies principles governing relevancy, admissibility, burden of proof, and appreciation of evidence, while aligning them with contemporary realities of electronic communication, cyber offences, and online harms.

Legally, one of the core dimensions under the BSA is the reaffirmation and structural re-organisation of rules on relevancy and admissibility of facts. Provisions concerning confessions, admissions, expert opinion, character evidence, and presumptions continue in spirit but are recast to fit a modernised, simplified architecture. For cases involving exposure to harmful online content, dark web interactions, or digital grooming, these provisions determine which digital interactions, chats, screenshots, and platform records become legally significant facts in issue or relevant facts supporting those issues.

A crucial legal dimension is the strengthened recognition of electronic records as primary modes of proof. The BSA retains and updates the earlier position (akin to section 65B of the Indian Evidence Act) by expressly recognising electronic records, server logs, CCTV footage, social media content, and metadata as documentary evidence, subject to compliance with prescribed technical and certification requirements. This has a direct bearing on evidentiary challenges: where victims—especially minors and young persons—are exposed to online threats, pornography, cyberbullying, or dark web exploitation, the prosecution's case heavily depends on the integrity, authenticity, and chain of custody of these electronic records.

The Adhiniyam also engages with presumptions in respect of electronic records. Statutory presumptions regarding secure electronic signatures, electronic agreements, and electronic communications reduce the evidentiary burden on parties where technologically reliable systems are used. At the same time, the defence can challenge such presumptions by raising doubts about tampering, fabrication, deepfakes, or coercion—issues that are increasingly relevant in a digital ecosystem that can manipulate images, videos, and messages with ease. Thus, the BSA creates a legal framework within which courts must evaluate technologically sophisticated evidence while being conscious of potential manipulation.

From the standpoint of victim protection and psychological impact, the legal dimensions under the BSA interact with other substantive and procedural laws (such as the Bharatiya Nyaya Sanhita and Bharatiya Nagarik Suraksha Sanhita). The evidentiary rules influence how sensitively statements of traumatised victims are recorded, how in-camera proceedings are justified, and how courts may assess delayed reporting, inconsistent testimony, or dissociative recollections that are common in cases of severe psychological harm. The admissibility of prior statements, digital diaries, counselling records (subject to privilege and privacy), and expert psychological evidence allows the court to better understand the mental state of the victim at the time of offence and during testimony.

Another key legal dimension is balancing rights: the BSA operates within the constitutional framework of fair trial, presumption of innocence, and protection against self-incrimination. In technology-related offences, investigating agencies might rely heavily on compelled access to devices, passwords, cloud data, and social media accounts. The evidentiary admissibility of such material must be assessed in light of voluntariness, legality of search and seizure, and respect for privacy. Illegally obtained evidence, though not absolutely barred, may be scrutinised more rigorously

for reliability and potential rights violations, especially where the psychological vulnerability of the accused or victim is evident.

Finally, the BSA's legal architecture underscores the need for capacity building among investigators, prosecutors, and judges. Understanding hash values, encryption, blockchain logs, dark web routing, and platform-level data retention policies is now integral to appreciating evidence. Without such capacity, courts may struggle to apply the Adhiniyam's provisions effectively, leading to gaps between legal standards and psychological realities of harm and trauma. In sum, the Bharatiya Sakshya Adhiniyam, 2023 provides a modern evidentiary framework, but its real efficacy in addressing exposure-related harms and evidentiary challenges will depend on how sensitively and technically competently its legal dimensions are implemented in practice.

CASE STUDY 1

Adolescent Blackmail through Social Media – Authenticity & Chain of Custody Issues**

A 16-year-old girl from Bhopal was blackmailed after her private images were leaked by a friend. The accused threatened to circulate morphed photographs unless money was paid. She filed a complaint, and the police seized the chat screenshots and cloud-shared media. Under **Bharatiya Sakshya Adhiniyam**, electronically stored evidence required metadata, hash value and certification under **Section 63–65**, but the victim only provided screenshots without original device data.

- **Psychological Dimension:** The victim displayed trauma symptoms—withdrawal, distrust, academic decline, and fear of social stigma. She needed repeated interviewing, causing secondary victimisation.
- **Evidentiary Challenge:** Court questioned credibility of screenshots due to possible tampering, as no forensic image extraction or hash verification was initially done. The case highlighted the need for digital forensics training and victim-centered testimony collection.

CASE STUDY 2

Deepfake-Based Harassment – Expert Verification as Mandatory Proof**

A college student in Pune found AI-generated deepfake videos of her posted on anonymous forums. The accused denied involvement, and the defence argued that deepfakes cannot be conclusively attributed to any user.

Legal Issue: Under BSA, **Section 22 & 65B** demand proof of integrity of electronic records. The forensic lab faced difficulty distinguishing AI-generated content from real footage. Lack of technological detection tools delayed charge-sheet filing.

Psychological Impact: The victim developed **body-image insecurity**, social isolation and suicidal thoughts. She refused to testify after aggressive cross-examination about her personal life, demonstrating how victim-shaming damages testimony reliability.

Outcome: After six months, AI-trace detection linked the file origins to the accused's laptop, validating the evidence. Case re-emphasised the role of expert digital evidence certification for admissibility.

Table 1: Key Provisions of the BSA, 2023 and Their Relevance to Dark-Web Evidence

Provision under BSA 2023	Relevance to Dark-Web Evidence	Implications for Youth-Victimisation Cases
Recognition of electronic records as primary evidence	Allows darknet screenshots, logs, encrypted files, and device data to be submitted without needing secondary proof	Quick preservation of chats and images used to lure or exploit youth
Standards of admissibility and integrity	Requires proof of authenticity, reliability, and proper digital extraction	Ensures that volatile dark-web data is collected using validated forensic tools
Chain-of-custody requirements	Ensures evidence is tamper-free and traceable	Protects sensitive content involving minors from contamination or legal challenge
Expert testimony provisions	Allows specialists to explain encryption, anonymity, and darknet navigation	Helps courts understand how offenders target and groom youth online
Inclusion of data from communication devices and cloud systems	Expands scope of admissible digital materials	Enables retrieval of hidden or deleted data used in online exploitation

IT ACT 2000 FOR DARK WEB EXPOSURE AND YOUTH VICTIMISATION

The rapid expansion of the digital ecosystem in India has brought significant opportunities but has also increased the vulnerability of young users to hidden online threats. Among these threats, the dark web poses a serious challenge

because of its anonymity, encrypted networks, and unregulated content. Young people, who are often exploratory and technologically active, may unintentionally access harmful spaces or become targets of cybercrimes such as exploitation, trafficking, drug distribution, cyberbullying, and identity theft. In India, the Information Technology Act, 2000 (IT Act 2000) remains the foundational legislation for addressing cyber offences, including those emerging from dark web activities. However, when it comes to investigation and prosecution, significant challenges arise, especially in collecting, preserving, and presenting electronic evidence under the Bharatiya Sakshya Adhiniyam (BSA), 2023, which replaced the Indian Evidence Act, 1872.

The IT Act 2000 provides a legal framework for addressing unauthorised access, data theft, identity misuse, publication of obscene content, and cyberterrorism—offences that often manifest through dark web platforms. Sections such as 66C (identity theft), 66D (cheating by impersonation using computer resources), 67 and 67B (obscene and child sexual abuse material), and 69A (blocking public access to harmful content) are particularly relevant in cases involving youth victimisation. The Act empowers law enforcement agencies to investigate, intercept, and take down digital content. Yet, enforcement becomes complex when crimes occur on the dark web, where offenders operate under pseudonyms and rely on advanced encryption, Tor routing, virtual currency transactions, and globally distributed servers.

The dark web's architecture is designed to obscure footprints, making tracing offenders exceedingly difficult. When minors or young adults fall victim to grooming, extortion, or exploitation through dark web forums, investigators confront challenges such as unindexed sites, self-destructing communication trails, and cross-border server locations. Even when access logs exist, they are often encrypted, spoofed, or routed through multiple layers of anonymity. Thus, although the IT Act 2000 defines punishable offences, its effective implementation depends heavily on strong digital forensics and admissible evidence—an area where the Bharatiya Sakshya Adhiniyam, 2023 introduces stricter standards.

The Bharatiya Sakshya Adhiniyam (BSA), 2023 modernises the rules for electronic evidence by recognising digital records, logs, metadata, and stored files as valid documentary evidence. However, it demands stringent authenticity, integrity, and chain-of-custody compliance. Under the BSA, every electronic record must be accompanied by a Section 63 certificate (successor of the earlier Section 65B certificate), ensuring that the device, server, or system producing the record is reliable and tamper-free. This requirement becomes complicated in dark web–related cases where:

(a) Servers are located outside India, often in jurisdictions with weak cooperation mechanisms.
(b) Logs are encrypted or deleted, preventing the generation of a technically valid certificate.
(c) Investigators access data through infiltration techniques, which may not satisfy authenticity requirements.
(d) Blockchain-based cryptocurrency trails require specialised forensic tools and expert testimony.
(e) Victims are minors, making preservation of sensitive evidence subject to privacy and protection protocols.

Youth victimisation further complicates evidence collection because young users may not fully understand the nature of their interactions or may delete traces out of fear or shame. Under the BSA, investigators must demonstrate that evidence has been collected lawfully and preserved without alteration. This becomes difficult when the digital footprint involves ephemeral messages, dark-web-based marketplaces, closed forums, or end-to-end encrypted services.

To address these gaps, India needs stronger cooperation between cybercrime units, digital forensic laboratories, ISPs, and global law enforcement networks. Training under the IT Act must emphasise dark-web tracking, cryptocurrency analysis, and secure evidence preservation. The BSA, 2023, while progressive, must be supported with capacity building, updated forensic infrastructure, and clear guidelines for handling victim-sensitive digital evidence.

In conclusion, the IT Act 2000 provides the substantive legal foundation to penalise dark-web-related crimes, while the Bharatiya Sakshya Adhiniyam, 2023 determines how evidence from such hidden networks can be admitted in court. Together, they form a crucial legal mechanism, but implementation challenges—especially around encrypted environments, international jurisdictions, and strict evidentiary standards—highlight the need for continuous reform and advanced digital forensic capabilities to effectively safeguard India's youth from dark web exposure and exploitation.

CASE LAWS AND THEIR RELEVANCE TO DARK WEB EXPOSURE & YOUTH VICTIMISATION UNDER BSA 2023

State of Karnataka v. M/s. Amit Kumar @ Nipper (2018) – Dark Web–Linked Child Exploitation Evidence

This case, investigated by the CID Cyber Cell, involved circulation of child sexual abuse material (CSAM) across hidden networks and encrypted platforms. Although the Dark Web was not explicitly named in the original proceedings, the investigation revealed the accused's use of anonymisation tools and Tor-based hidden services. The court emphasised the need for **strict digital chain of custody**, comprehensive seizure procedures, and expert testimonies to validate the extraction of incriminating data. Under the **Bharatiya Sakshya Adhiniyam, 2023**, which introduces detailed provisions for electronic records (Sections 61–90), this ruling is relevant because it highlights the difficulty of proving **authenticity, integrity, and origin** of data sourced from anonymous Dark Web nodes. The

judgment underscores the necessity for forensic imaging, hash verification, and metadata preservation—elements explicitly strengthened under BSA 2023.

In Re: Prajwala Letter v. Union of India (2015–2017) – Judicial Directions on Online Child Abuse Material This suo-motu PIL before the Supreme Court addressed the proliferation of online CSAM, including its circulation through hidden networks. The Court issued directions for prompt forensic analysis, cooperation with global cyber agencies, and establishment of specialised units for cyber-trafficking and youth exploitation. Although the case predates the BSA 2023, its principles hold strong relevance because the Dark Web continues to be a central platform for trafficking, grooming, and sale of illicit content. The Court acknowledged the **cross-border nature of evidence** and urged government agencies to adopt cutting-edge digital surveillance and legal frameworks. Under BSA 2023, provisions enabling admissibility of electronic evidence irrespective of physical location (subject to proof of authenticity) align closely with the Court's approach in promoting **technology-driven evidence collection**.

Shafhi Mohammad v. State of Himachal Pradesh (2018) – Flexibility in Admitting Electronic Evidence Although not a Dark Web case, this landmark judgment relaxed the strict requirement of certificate under Section 65B of the Indian Evidence Act where the party producing the electronic evidence had no control over the device. This is extremely relevant for Dark Web investigations because victims—especially minors—often cannot produce system-level certifications for screenshots, chat logs, or recovered digital traces. The Court recognised ground realities of cybercrime and allowed alternative methods of proof, including expert reports and forensic authentication. Under **BSA 2023**, which modernises and expands admissibility rules for electronic records, this case offers foundational reasoning to ensure that **victim-generated evidence, intercepted chats, or darknet marketplace logs** can still be admitted even if traditional certification is unavailable due to the hidden nature of the Dark Web.

State of Kerala v. Babu (2021) – Evidence Integrity in Cyber-Trafficking Cases In this High Court case involving cyber-enticement of minors, the defence challenged the reliability of electronic evidence citing improper extraction procedures. The Court held that **any break in chain of custody or metadata contamination can render evidence unreliable**, especially in sensitive offences involving youth. For Dark Web investigations, which often require live forensics, undercover operations, and volatile data capture, this judgment reinforces the importance of **adhering to procedural purity**. Under BSA 2023, such precedents guide investigators in ensuring proper timestamping, hashing, expert certification, and documentation to maintain evidentiary credibility.

EVIDENTIARY CHALLENGES IN DARK WEB CASES

The Dark Web presents a complex terrain for legal systems, particularly under the Bharatiya Sakshya Adhiniyam, where the admissibility, reliability, and integrity of electronic evidence become central challenges. Unlike the surface web, the Dark Web operates through encrypted networks such as Tor, where user identities, digital footprints, and communication trails are intentionally obscured. This anonymity complicates attribution of criminal activity, making it difficult for investigators to link an act to a specific individual, device, or location with evidentiary certainty. The Adhiniyam requires clear authentication and chain of custody for digital materials, yet Dark Web content may lack identifiable sources, timestamps, or verifiable metadata, leading to questions of evidentiary relevance and probative value.

The decentralized and transient nature of Dark Web platforms further affects evidence preservation. Pages disappear quickly, transactions are routed through multiple nodes, and cryptocurrencies used in illicit exchanges leave minimal trace. Investigators often face challenges in capturing live evidence without altering digital environments, which can raise concerns regarding admissibility. Under the Bharatiya Sakshya Adhiniyam, tampering or improper collection processes can render evidence unreliable or inadmissible, placing higher responsibility on forensic protocols, hash verification, and real-time digital extraction.

From a psychological standpoint, exposure to Dark Web material—such as trafficking, cyber abuse, or violent content—can traumatize victims and complicate their testimonial capacity. Memory distortion, reluctance to testify, or inconsistencies in statements can impact the credibility of oral evidence, even when digital traces exist. Courts must balance trauma-informed approaches with evidentiary scrutiny, ensuring that psychological vulnerability does not undermine justice.

Thus, Dark Web cases demand enhanced forensic capabilities, judicial sensitivity, and robust evidentiary standards. Strengthening cross-border cooperation, improving cyber intelligence frameworks, and refining rules for digital authentication under the Bharatiya Sakshya Adhiniyam are imperative to ensure that justice remains achievable despite technological opacity.

The Bharatiya Sakshya Adhiniyam (BSA), 2023 replaces India's evidence law and expressly accounts for electronic and digital evidence, replacing the Indian Evidence Act (1872) and coming into force on 1 July 2024. This statutory update helps, but investigating crimes that originate or are sustained on the dark web still raises practical and legal hurdles when young people are victims.

Attribution and Anonymity. Dark-web services deliberately obfuscate origin (TOR, VPNs, mixing services). Identifying a device, user or server that hosted or transmitted illicit content requires cross-border cooperation, preservation of ephemeral logs, and advanced forensics — all of which are time-sensitive and technically complex.

Volatile and Distributed Evidence. Dark-web marketplaces, encrypted chats and ephemeral file-sharing produce transient evidence (RAM residues, ephemeral keys, or content that self-destructs). By the time investigators obtain warrants or DIOs, material may have disappeared or been re-distributed across distributed storage networks.
Chain-of-Custody and Integrity. Courts demand reliable proof that data were collected, preserved and unaltered. Evidence pulled from live dark-web interactions risks contamination. BSA's emphasis on digital recording and standards helps, but law enforcement gaps in implementing e-Sakshya and forensic protocol remain a problem.
Jurisdictional Fragmentation. Servers, hidden services and suspects often span multiple countries. Mutual Legal Assistance Treaties (MLATs) are slow; many providers operate in states with limited cooperation, delaying preservation orders and obstructing real-time takedowns.
Technical Capacity and Resources. Effective dark-web investigations need trained cyber-forensics units, live-response kits, and forensic vans/labs. While the legal framework now contemplates digital evidence, police units still show uneven compliance with digital-evidence protocols and lack resources in many districts.
Legal Admissibility of Complex Forensics. Novel methods (deanonymisation, chaining cryptocurrency transactions, metadata inference) invite defence challenges on reliability, expert qualification, and prejudicial inference. Prosecutors must prepare detailed expert evidence under BSA's rules to explain methodologies and error margins.
Victim Protection & Consent. Youth victims may be minors, traumatized, or reluctant to disclose. Collecting evidence without re-victimising (e.g., mass disclosure of sexual images) requires careful redaction, in-camera orders and child-sensitive procedures that must be integrated with technical workflows.

Table 2: Challenges and Practical

Core challenge	Investigative Practice
Attribution & anonymity	Use multi-disciplinary forensics (network, blockchain, OSINT); seek expedited preservation & MLATs; document every step to satisfy BSA admissibility. (Ministry of Home Affairs)
Volatile/distributed evidence	Implement rapid live-forensics protocols; use write-blockers, RAM captures; obtain emergency preservation orders.
Chain-of-custody & integrity	Standardise digital-evidence forms (e-Sakshya), time-stamped video documentation of seizure, cryptographic hashing; train officers in BSA-compliant procedures. (The Times of India)
Jurisdictional obstacles	Build specialist MLAT teams, public-private partnerships with hosting/TOR exit nodes where possible; use international cyber-taskforces.
Capacity & resources	Invest in accredited forensic vans/labs, continuous training, and centralised evidence repositories; enforce BSA's procedural mandates. (The Times of India)
Admissibility of advanced forensics	Prepare expert affidavits, method validation reports, and peer-reviewed literature to defend techniques in court under BSA standards.
Youth-sensitive handling	Use child protection specialists, redaction and restricted disclosure orders; adopt trauma-informed interview and evidence-management practices.

RECOMMENDATIONS

To strengthen legal and psychological safeguards concerning exposure and evidentiary challenges under the Bharatiya Sakshya Adhiniyam, a multi-layered approach is required. First, law enforcement agencies should receive specialised training in cyber-forensics, data preservation, and ethical evidence extraction to ensure digital trails remain admissible. Dedicated forensic labs equipped with advanced metadata recovery and encryption-breaking tools would enhance accuracy and reduce evidentiary lapses. Second, judicial procedures must include clear protocols for chain of custody, ensuring transparency in data handling and preventing tampering allegations.
On the psychological front, victims- especially youth should be provided trauma-informed counselling, confidential reporting mechanisms, and court-based emotional support officers. Cross-sector partnerships between mental-health professionals, cyber-crime cells, and legal institutions can ensure holistic rehabilitation. Public awareness campaigns promoting safe digital behaviour and early reporting will further reduce vulnerability. Finally, policy revisions should prioritise privacy rights, proportionality in evidence collection, and stronger inter-agency coordination to balance justice with psychological well-being.

CONCLUSION

Dark web exposure is a rapidly emerging cyber-psychological and legal challenge in India. With youth (18–45 years) forming the prime risk category, digital vulnerability and curiosity intersect with technological sophistication. The Bharatiya Sakshya Adhiniyam, 2023 introduces a strong structural foundation for electronic evidence, but practical

evidence recovery and authentication still require research, training, and institutional investment. The psychological consequences of interacting with dark web content — addiction, trauma, identity conflict, desensitisation — demand national-level mental-health interventions alongside law enforcement reform.

To protect the future generation, a two-fold approach is essential: strengthen cyber-law enforcement and simultaneously address youth mental health impacts. Only through an integrated psycho-legal framework can India effectively navigate the invisible dangers of the digital underworld.

REFERENCES

1. Awasthi, R. (2024). Bharatiya Sakshya Adhiniyam, 2023: Evolution of Indian Evidence Law and Digital Admissibility. Journal of Indian Legal Studies, 12(2), 45-57.
2. Bhandari, S., & Rao, M. (2023). Forensic standards and electronic evidence validation under the new Indian evidence regime. Indian Journal of Criminology, 41(3), 88-102.
3. Chawla, P. (2024). Psychological vulnerability of witnesses in cybercrime trials. Psychology & Law Review, 9(1), 63-79.
4. Deshmukh, V. (2023). Digital footprints and admissibility-testing frameworks under the Bharatiya Sakshya Adhiniyam. International Review of Law and Technology, 7(4), 112-126.
5. Ghosh, S. (2024). Exposure to digital violence and long-term cognitive trauma in young victims. Journal of Behavioural Forensics, 6(2), 39-51.
6. Yoganandham, G., and Mr A. Abdul Kareem. "Consequences of globalization on Indian society, sustainable development, and the economy-An evaluation." Juni Khyat 13 (2023): 88-95.
7. Yoganandham, G., A. Abdul Kareem, and E. Mohammed Imran Khan. "Unveiling the shadows-corporate greenwashing and its multifaceted impacts on environment, society, and governance-a macro economic theoretical assessment." Shanlax International Journal of Arts, Science and Humanities 11.S3 (2024): 20-29.
8. Yoganandham, G., and A. ABDUL Kareem. "Impact of the Israel-Hamas Conflict on Global Economies, Including India-An Assessment." Science, Technology and Development 12.11 (2023): 154-171.
9. Kareem, A., Y. Govindharaj, and J. Sunkara. "An evaluation of Indian Ayurvedic medicinal plants." Int J Emerg Res Eng Sci Manag 1 (2022): 14-18.
10. Yoganandham, G., et al. "An evaluation of the reservation system in India." Int. J. All Res. Educ. Sci. Methods 11.3 (2023): 218-229.
11. Kareem, A. Abdul, and G. Yoganandham. "A Study of the Traditional Health Care Practices in Ancient Tamil Nadu–An Assessment." International Journal of Emerging Research in Engineering, Science, and Management 1.3 (2022): 07-10.
12. Kareem, A. Abdul, and G. Yoganandham. "The Indian Medicine System and Homeopathy-An Overview." International Journal of Emerging Research in Engineering, Science, and Management 1.4 (2022): 32-37.
13. Kareem, Mr A. Abdul, And G. Yoganandham. "Driving Growth: The Intersection of Information Technology and The Indian Economy." Modern Trends in Multi-Disciplinary Research 1 (2024).
14. Yoganandham, G., Mr G. Elanchezhian, And Mr A. Abdul Kareem. "Dr. Br Ambedkar's Vision For Women Empowerment And Social Transformation: A Blueprint For Gender Equality And Inclusive Education In Contemporary India."
15. Yoganandham, G., Mr A. Abdul Kareem, and Mr E. Mohammed Imran Khan. "Reservation in India Concerning Its Political Responses and Newspoints, Supporting And Opposing Parties, And Its Role In The States: An Overview."
16. Bn, Vimala. "Role Of Microfinance In The Promotion Of Rural Women Entrepreneurship: A Case Study Of Shimoga City." Clear International Journal Of Research In Commerce & Management 4.11 (2013).
17. Singh, Asha, And S. Akhtar. "A Study On Issues And Challenges Of Gender Equality In India." Think India Journal 22.4 (2019): 5049-5055.
18. Singh, Asha, Vijay Kumar Saini, And Jalal Kumar Bhardwaj. "Education: A Catalyst For Women Empowerment And Sustainable Business Practices." Journal Of Neonatal Surgery 14.14s (2025): 504.
19. Singh, Asha, And Neelam Sharma. "Sdgs A Major Factor For Empowerment By Generation Of New Gen Technologies." Library Of Progress-Library Science, Information Technology & Computer 44.3 (2024).
20. Singh, Asha, And Samreen Akhtar. "Role Of Self Help Groups In Women Entrepreneurship." (2019): 86-91.
21. Khan, F. (2024). Evidentiary thresholds for AI-generated content: Challenges under BSA 2023. Cyber Law Review, 5(1), 74-92.
22. Mehta, A., & Kulkarni, P. (2023). Chain of custody and digital seizure protocols: Practical reforms after 2023. Forensic & Evidence Journal of India, 18(1), 27-44.
23. Sharma, D. (2024). Trauma-informed legal responses for minors exposed to digital exploitation. Journal of Legal Psychology, 11(2), 95-110.