International Research Journal of Multidisciplinary Scope (IRJMS), 2026; 7(3): 49-58 IRJMS

Original Article | ISSN (O): 2582-631X DOI: 10.47857/irjms.2026.v07i03.012119

Dark Web and Criminal Liability in India

Kriti Singh[1]*, Gouri Malhotra[1], Gaurav Kumar[2]

[1]Amity School of Communication, Amity University, Noida, Uttar Pradesh, India, [2]School of Law, IILM University, Greater Noida, Uttar Pradesh, India. *Corresponding Author's Email: ksingh21@amity.edu

Abstract

The rapid advancement of digital technologies has led to the emergence of the dark web as a distinct and anonymised segment of the internet, raising significant concerns within the domain of cyber law and criminal liability. While existing scholarship has examined cybercrime broadly, there remains limited doctrinal analysis specifically addressing dark web-related legal challenges within the Indian legal framework, a gap this study seeks to address. The study aims to examine the legal dimensions of activities associated with the dark web within the framework of Indian cyber and criminal law. The research adopts a doctrinal and analytical methodology, relying on statutory provisions, judicial decisions, and academic literature to evaluate the applicability of existing legal frameworks. The findings indicate that while the Information Technology Act, 2000, the Bharatiya Nyaya Sanhita, 2023, and evidentiary laws provide a foundational basis for addressing cyber offences, their application in anonymised and decentralised digital environments presents significant interpretative and practical challenges. Key issues identified include difficulties in attribution of liability, jurisdictional limitations in cross-border offences, and constraints in the collection and admissibility of digital evidence. The study further highlights that enforcement challenges, including limitations in forensic infrastructure and dependence on international cooperation mechanisms, significantly affect the effectiveness of legal responses. It is concluded that effective regulation of dark web-related activities requires a coordinated approach involving legislative reform, institutional capacity building, and technological integration to ensure robust cybercrime governance in India.

Keywords: Criminal Liability, Cybercrime, Cyber Law Enforcement, Dark Web, Digital Evidence.

Introduction

The rapid advancement of digital technologies has given rise to new and complex digital environments, among which the dark web represents a particularly distinct and challenging domain. Functioning through encrypted networks and specialised protocols, the dark web enables a high degree of user anonymity and secure data exchange, thereby differentiating itself from the surface web that is accessible through conventional search engines (1). Scholarly discourse has increasingly examined the structural and functional dimensions of the dark web, particularly its role in facilitating both legitimate and illicit activities. On one hand, it serves as a platform for privacy protection, secure communication, and information exchange in contexts such as whistleblowing and political dissent. On the other hand, it has been associated with cybercrime, including illegal trade, data breaches, financial fraud, and other forms of digital misconduct (2, 3). For the purposes of this study, dark web-related activities are understood to encompass three distinct categories: legitimate anonymous usage, including privacy protection and secure communication; cybercriminal operations, including illegal trade, financial fraud, and data breaches; and unauthorised transactions conducted through anonymous platforms beyond the reach of conventional regulatory oversight. Studies have highlighted that anonymity and encryption embedded within dark web infrastructures significantly complicate regulatory oversight and law enforcement efforts (1, 2). From a legal perspective, the emergence of such anonymised digital environments poses significant challenges to traditional frameworks of criminal liability, which are typically premised on identifiable actors, clearly attributable conduct, and territorially bounded jurisdiction. Existing literature in cyber law suggests that the application of conventional legal principles to digital contexts requires careful adaptation, especially in relation to issues of intent, participation, and evidentiary standards in cyberspace (4). The complexity of digital evidence, including its collection, preservation, and admissibility, further adds to the

(Received 01st May 2026; Accepted 09th June 2026; Published 01st July 2026)

challenges faced by legal systems in addressing cyber offences effectively (5). In the Indian context, the legal framework governing cyber activities is primarily anchored in the Information Technology Act, 2000, supplemented by provisions of the Indian Penal Code, 1860, now replaced by the Bharatiya Nyaya Sanhita, 2023 (6), along with relevant evidentiary laws. While these legal instruments provide a foundational structure for regulating cyber offences, they were developed in a technological environment that did not fully anticipate the rise of anonymised and decentralised networks such as the dark web (7, 8). Consequently, their application in such contexts raises concerns regarding the adequacy of existing provisions in addressing issues of attribution, jurisdiction, digital evidence, and enforcement.

The challenges posed by the dark web are further intensified by its cross-border nature, which often involves multiple jurisdictions and necessitates reliance on international cooperation mechanisms. Scholarly analyses have pointed out that delays in mutual legal assistance processes, coupled with differences in national legal frameworks, may hinder effective investigation and prosecution of cyber offences (9, 10). At the international level, instruments such as the Budapest Convention on Cybercrime, 2001 (11), and the European Union Directive on Attacks Against Information Systems (2013/40/EU) represent attempts to address these challenges through harmonised regulatory frameworks. At the same time, limitations in forensic infrastructure, technical expertise, and institutional capacity continue to affect the practical implementation of cyber laws, particularly in complex digital environments.

Against this backdrop, the research objective of the present study is to examine the legal dimensions of activities associated with the dark web within the framework of Indian cyber and criminal law. The study seeks to analyse the nature and functioning of the dark web, evaluate the structure of criminal liability under Indian law, assess the applicability of existing legal provisions in addressing issues such as attribution, jurisdiction, and digital evidence, and identify key legal gaps and enforcement challenges in regulating such activities. The selection of statutory provisions and judicial precedents examined in this study is informed by their direct relevance to the identified research questions, their foundational significance within the Indian cyber and criminal law framework, and their applicability to the regulatory challenges posed by anonymised digital environments.

In this context, the study addresses the following research questions:

RQ1: What is the nature and functioning of the dark web in contemporary digital environments?

RQ2: How is criminal liability structured under Indian law in relation to cyber activities?

RQ3: To what extent are existing legal provisions adequate in addressing activities associated with the dark web, particularly with respect to attribution, jurisdiction, and digital evidence?

RQ4: What are the key legal and enforcement challenges in regulating dark web-related activities in India?

Implications and Contributions

This study contributes to the doctrinal legal scholarship on cybercrime regulation in India by providing a structured analysis of the nature and functioning of the dark web, the framework of criminal liability under Indian law, and the adequacy of existing legal provisions in addressing attribution, jurisdiction, and digital evidence in anonymised digital environments. The findings carry implications for legislative reform, particularly in relation to the Information Technology Act, 2000 and the Bharatiya Nyaya Sanhita, 2023, and for strengthening institutional and forensic capacities of enforcement agencies. The study further contributes to policy discourse on international cooperation mechanisms, including Mutual Legal Assistance Treaties (MLAT), in the context of transnational cybercrime. It is anticipated that the analysis will be of relevance to legal scholars, policymakers, and enforcement agencies engaged with cybercrime regulation in India and the broader Global South.

Methodology

Research Design

This study adopts a doctrinal and analytical research methodology, focusing on the examination and interpretation of legal principles governing activities associated with the dark web within the framework of Indian law. The primary emphasis is on analysing the concept of criminal liability in cyber environments, particularly in the context of challenges arising from anonymised digital settings.

The research is descriptive and analytical in nature. It explains the functioning of the dark web while assessing the adequacy of existing legal provisions. The study does not involve empirical investigation and is based on legal reasoning to examine issues relating to criminal liability, jurisdiction, and evidentiary standards. The doctrinal methodology employed in this study involves three analytical steps: first, identification of relevant statutory provisions and judicial precedents; second, systematic interpretation of these sources in light of the regulatory challenges posed by the dark web; and third, critical evaluation of the adequacy of existing legal frameworks against identified gaps and enforcement challenges.

Sources of Data

This study is based on secondary data sources, including statutory provisions, judicial precedents, and academic literature. The primary legal framework examined comprises the Information Technology Act, 2000, along with relevant provisions of the Bharatiya Nyaya Sanhita, 2023 (6), and other applicable laws governing cyber activities in India. These statutes were selected on the basis of their foundational and operative significance within India's cyber and criminal law framework, their direct applicability to the offence categories most commonly associated with dark web activity, and their centrality to existing judicial interpretation of digital offences in India.

Judicial decisions of Indian courts are analysed to understand the interpretation and application of cyber law and criminal liability. Key cases include

a) Shreya Singhal v. Union of India (12),
b) Anvar P.V. v. P.K. Basheer (5),
c) Avnish Bajaj v. State (N.C.T.) of Delhi (13), and
d) K.S. Puttaswamy v. Union of India (14).

These cases were selected on the basis of the following criteria: their direct relevance to the intersection of digital technology and criminal or constitutional law; their authoritative status as Supreme Court or High Court decisions that have shaped the interpretation of cyber law in India; and their specific applicability to the issues of digital evidence, intermediary liability, free expression, and the right to privacy —each of which has direct bearing on the regulatory challenges examined in this study.

The study also incorporates secondary academic sources, including books, peer-reviewed journal articles, and policy reports, to provide conceptual clarity and contextual understanding.

Scope of the Study

The study is confined to the Indian legal system, with particular focus on the applicability of cyber and criminal laws to activities associated with the dark web. It examines issues relating to criminal liability, jurisdiction, attribution, and digital evidence within anonymised digital environments. Limited reference to international perspectives is made only for conceptual clarity.

Limitations

The study is based exclusively on secondary sources and does not involve primary or empirical data collection. It adopts a doctrinal approach, focusing on legal interpretation rather than field-based investigation. The anonymous nature of the dark web limits the availability of verifiable case-specific information. The scope is restricted to the Indian legal framework and does not include detailed comparative analysis or access to confidential enforcement data. More broadly, doctrinal legal research carries inherent epistemological limitations that warrant acknowledgement. As a methodology, it relies on the interpretation of authoritative legal texts and judicial reasoning, and does not engage with the lived realities of enforcement, the experiences of affected individuals, or empirically verifiable data on the prevalence and nature of dark web-related offences. The findings of this study are therefore interpretive and analytical in nature, and should be understood as contributions to legal scholarship rather than as empirical determinations of fact. Additionally, the rapidly evolving technological landscape of the dark web means that legal analysis conducted at a given point in time may require periodic revision as new judicial interpretations, legislative developments, or technological changes emerge. These limitations are acknowledged as inherent to the methodology adopted and do not diminish the scholarly value of the doctrinal approach in identifying legal gaps and informing policy discourse.

Results

The present study, based on doctrinal analysis of statutory provisions, judicial decisions, and relevant academic literature, yields the following findings:

Nature of the Dark Web

The dark web operates as an anonymised and encrypted segment of the internet, characterised by decentralisation and restricted accessibility. Existing scholarship on hidden internet structures highlights that such environments limit traceability and user identification, thereby complicating regulatory oversight and legal intervention (1). The dual-use nature of such networks is recognised in academic discourse, where legitimate uses — including privacy protection and secure communication — coexist with activities that may raise concerns under cybercrime frameworks (2, 3). Specifically, dark web activities may be categorised as: first, legitimate anonymous usage by journalists, whistle-blowers, and privacy-conscious individuals; second, cybercriminal operations including drug trafficking, weapons trade, and financial fraud; and third, unauthorised transactions on anonymous platforms involving stolen data, malware, and illicit services. This tripartite distinction is significant from a doctrinal standpoint, as the legal response to each category requires a different regulatory approach under Indian law. This duality presents a regulatory challenge, as Indian law does not distinguish between lawful and unlawful use of anonymisation technologies, creating interpretative ambiguity in the application of existing provisions.

Challenges to Traditional Criminal Liability

The study finds that traditional principles of criminal liability — premised on identifiable actors, attributable conduct, and clearly established intent — encounter significant interpretative challenges in anonymised digital environments. The Bharatiya Nyaya Sanhita, 2023 (6), like its predecessor the Indian Penal Code, 1860, does not contain provisions specifically addressing offences committed through anonymised networks. Contemporary cyber law scholarship emphasises that attribution of intent and participation becomes complex in decentralised and encrypted networks, requiring adaptive interpretation of legal doctrines (4). The absence of explicit statutory guidance on anonymised environments indicates a legislative gap that may affect the effectiveness of criminal prosecution in dark web-related cases.

Limitations of the Existing Legal Framework

The Information Technology Act, 2000 provides the primary statutory basis for addressing cyber offences in India. However, the Act was enacted in a technological context that did not anticipate anonymised and decentralised network architectures such as the dark web. Section 66 of the IT Act, which addresses computer-related offences, and Section 67, which governs obscene material in electronic form, do not contain provisions specifically addressing attribution difficulties in anonymised environments. Section 66A, which was struck down in Shreya Singhal v. Union of India (2015) 5 SCC 1 (12) on grounds of unconstitutional vagueness, and Section 66B, which addresses receiving stolen computer resources, similarly reflect the limitations of a legislative framework that did not anticipate the structural complexity of anonymised networks (15). Recent doctrinal analyses of India's cyber law framework highlight accountability gaps, regulatory limitations, and challenges in addressing emerging forms of cybercrime within such digital ecosystems (8, 16, 17). These gaps suggest that the existing framework may require legislative clarification to remain effective in the context of evolving digital threats.

Attribution and Jurisdictional Constraints

Attribution remains a critical doctrinal challenge due to the use of anonymisation technologies and decentralised infrastructures inherent in dark web operations. Under Indian law, establishing criminal liability requires proof of identity and direct linkage between an accused and a specific act — a standard that anonymised environments significantly complicate. Literature on cross-border cybercrime and international law highlights those jurisdictional complexities arise when offences span multiple legal systems, often limiting effective enforcement (10, 18, 19). The IT Act, 2000 does not contain an explicit effects-based jurisdictional provision capable of addressing

offences originating outside Indian territory through anonymous networks, further limiting the reach of Indian law in cross-border dark web cases.

Evidentiary Challenges

The admissibility of digital evidence in Indian courts is governed by the Indian Evidence Act, 1872, as amended, and subsequently by the Bharatiya Sakshya Adhiniyam, 2023 (20). The Supreme Court in Anvar P.V. v. P.K. Basheer (2014) 10 SCC 473 reinforced the importance of procedural compliance and certification requirements for electronic records (4). However, evidence originating from dark web environments presents particular challenges, as the anonymised and encrypted nature of such networks complicates the establishment of authenticity and integrity of digital records. Contemporary research on digital forensics and evidentiary practices highlights practical challenges in collection, preservation, and admissibility of such evidence, particularly in anonymised environments (21, 22). This indicates a gap between existing evidentiary standards and the practical realities of dark web investigations.

Enforcement and Investigative Limitations

The study identifies significant practical constraints in enforcement, including limitations in forensic infrastructure, technical expertise, and investigative capacity among Indian law enforcement agencies. Research on cybercrime policing and investigation suggests that agencies face increasing difficulty in tracking offenders within encrypted and decentralised networks (23, 24). These limitations are further compounded by the absence of a dedicated institutional framework for dark web investigations in India, and indicate that legislative reform alone may be insufficient without corresponding institutional capacity building.

Dependence on International Cooperation

Cybercrime involving the dark web frequently requires cross-border cooperation due to the transnational nature of such networks. India's primary mechanism for international legal cooperation in criminal matters is the Mutual Legal Assistance Treaty (MLAT) framework. Literature on transnational cybercrime indicates that MLAT mechanisms are often constrained by procedural delays, jurisdictional limitations, and coordination challenges, affecting timely investigation and prosecution (9, 18). India has entered into MLATs with a limited number of jurisdictions, and the absence of comprehensive bilateral arrangements with key technology-hosting countries may further limit the effectiveness of cross-border enforcement in dark web cases.

Structural Gap Between Technology, Law and Enforcement

The study identifies a broader structural gap between technological advancements, existing legal frameworks, and enforcement capabilities in the Indian context. The IT Act, 2000 and the Bharatiya Nyaya Sanhita, 2023, while providing a foundational legal basis, were not designed to address the specific regulatory challenges posed by anonymised and decentralised digital environments. Scholarly work suggests that this misalignment results in regulatory inefficiencies, particularly in rapidly evolving digital environments where technological developments outpace legal adaptation (4, 16, 19). This structural gap indicates the need for a coordinated legislative, institutional, and technological response to ensure effective cybercrime governance in India.

Summary of Findings

The effectiveness of criminal liability in regulating dark web-related activities in India is shaped by the interaction of technological anonymity, evolving legal frameworks, and enforcement limitations. The doctrinal analysis indicates that while foundational legal provisions exist, specific legislative gaps in attribution, jurisdiction, evidentiary standards, and institutional capacity may significantly limit their practical effectiveness. This indicates the need for adaptive, coordinated, and technologically informed regulatory approaches.

Discussion

The findings of the present study collectively indicate that the Indian legal framework, while providing a foundational basis for addressing cyber offences, confronts significant interpretative and structural challenges in the specific context of dark web-related activities. The structural features of anonymised and decentralised networks — including encryption, restricted traceability, and cross-border operation — do not map neatly onto the attribution-based premises of criminal liability

under either the Bharatiya Nyaya Sanhita, 2023, or the Information Technology Act, 2000. This misalignment suggests that existing legal provisions, though applicable in principle, may require purposive and adaptive judicial interpretation in the absence of targeted legislative reform (4, 6). These findings are broadly consistent with earlier scholarship on the limitations of conventional criminal law frameworks in digital environments. It has been argued in past research that criminal liability doctrines premised on physical presence and identifiable actors require fundamental reconceptualisation in cyberspace (4), a position that the present study's doctrinal analysis affirms specifically in the context of anonymised dark web environments. Similarly, comparable accountability gaps in India's cyber law framework have been identified in past studies (8, 16), and the present study extends these observations by grounding them in a systematic analysis of specific statutory provisions and their interpretive limitations.

The dual-use nature of the dark web presents a further doctrinal complexity. As scholarship has recognised, anonymisation technologies serve both legitimate and potentially unlawful purposes (2). Any regulatory response must therefore be proportionate and carefully calibrated to avoid the unintended consequence of criminalising privacy-protective conduct. The Supreme Court's recognition of the right to privacy as a fundamental right in K.S. Puttaswamy v. Union of India (2017) 10 SCC 1 is particularly significant in this context, as it suggests that regulatory measures targeting anonymised networks must satisfy the tests of legality, necessity, and proportionality established by the Court (14). This constitutional constraint distinguishes India's regulatory context from jurisdictions such as the United Kingdom, where the Investigatory Powers Act 2016 permits broader surveillance authority, and the European Union, where the General Data Protection Regulation (GDPR) creates a parallel framework of data rights that coexists with cybercrime enforcement. The tension between privacy rights and regulatory imperatives identified in this study reflects a structural challenge that comparative scholarship has also noted in other democratic jurisdictions (9). This constitutional dimension introduces an important constraint on the scope of permissible legislative intervention in the dark web domain.

The study's findings regarding legislative gaps in attribution, jurisdiction, and evidentiary standards are consistent with observations in comparative legal scholarship (8, 16). Jurisdictions such as the United Kingdom, through the Computer Misuse Act 1990 as amended, and the European Union, through the Directive on Attacks Against Information Systems (2013/40/EU), have developed more targeted legislative instruments addressing cybercrime in anonymised environments. The Budapest Convention on Cybercrime, 2001 (11), to which India is not a signatory, provides an internationally recognised framework for harmonising cybercrime laws and facilitating cross-border cooperation (9). A comparison of India's legal framework with the Budapest Convention reveals three specific areas of divergence: first, the absence of an effects-based jurisdictional clause in the IT Act, 2000, which contrasts with Article 22 of the Budapest Convention; second, the absence of provisions specifically addressing offences committed through anonymised networks, which the Convention addresses through its substantive offence provisions; and third, India's limited bilateral cybercrime cooperation architecture, which contrasts with the Convention's established mutual assistance framework. These divergences are not merely technical — they represent structural gaps that may materially affect India's capacity to investigate and prosecute dark web offences with cross-border dimensions. India's non-accession to the Budapest Convention may be noted as a structural factor that limits the availability of established international cooperation mechanisms, including the enhanced cooperation framework established under the Second Additional Protocol to the Budapest Convention (25), though this requires careful contextualisation given India's stated concerns regarding data sovereignty and jurisdictional autonomy.

The certification requirements for electronic evidence established in Anvar P.V. v. P.K. Basheer (2014) 10 SCC 473, while procedurally sound, may present practical challenges in dark web investigations where the chain of digital custody is inherently difficult to establish (5, 21). Earlier scholarship has similarly noted practical

limitations in the application of evidentiary standards to digital environments (21, 22), and the present study reinforces these observations by identifying the specific challenges posed by the anonymised and encrypted nature of dark web evidence. The gap between existing evidentiary standards and the practical demands of dark web investigations thus represents not merely a technical problem but a structural misalignment between the legal framework and the technological realities it seeks to govern.

The enforcement challenges identified in this study suggest that legal reform alone may be insufficient to address dark web-related cybercrime effectively. Research indicates that law enforcement agencies require specialised forensic capabilities and institutional frameworks to investigate offences in anonymised digital environments. Significant gaps in India's cybercrime policing infrastructure have been identified in past research (23, 24), and the present study's findings corroborate these observations while extending them to the specific context of dark web investigations. The absence of a dedicated institutional framework for dark web investigations represents a gap that legislative reform alone cannot address — it requires a coordinated investment in technical capacity, training, and inter-agency coordination. The dependence on MLAT mechanisms for cross-border cooperation presents a further structural concern. The procedural delays and jurisdictional limitations associated with existing MLAT frameworks (9, 18) suggest the need for more streamlined bilateral arrangements, particularly with jurisdictions that host significant dark web infrastructure.

A recurring theme in the analysis is the tension between effective regulation of dark web activities and the protection of legitimate uses of privacy-enhancing technologies (2, 4). This tension is not unique to India — it reflects a broader global challenge in cybercrime governance. The study suggests that an adaptive regulatory approach — one that integrates targeted legislative amendments, institutional capacity building, and technologically informed enforcement practices — may offer a more sustainable framework for addressing dark web-related criminal activity than broad prohibitory measures. Such an approach would need to remain consistent with constitutional guarantees of privacy and expression, and with India's obligations under international human rights frameworks (14).

Conclusion

This study set out to examine the legal dimensions of activities associated with the dark web within the framework of Indian cyber and criminal law, with specific focus on four dimensions: the nature and functioning of the dark web, the structure of criminal liability under Indian law, the adequacy of existing legal provisions in addressing attribution, jurisdiction, and digital evidence, and the key enforcement challenges facing regulatory authorities. Employing a doctrinal and analytical methodology, the study drew on statutory provisions, judicial precedents, and academic literature to systematically evaluate these dimensions and identify areas requiring legislative, institutional, and policy attention.

The analysis indicates that while the existing legal framework — comprising the Information Technology Act, 2000, the Bharatiya Nyaya Sanhita, 2023, and applicable evidentiary laws — provides a foundational basis for addressing cyber offences, its application in anonymised and decentralised digital environments presents significant practical and interpretative challenges.

The study's findings yield the following doctrinal conclusions. First, the dark web's architecture of anonymity, encryption, and decentralisation distinguishes it fundamentally from conventional digital environments and limits the applicability of standard regulatory and evidentiary frameworks. Second, the principles of criminal liability under Indian law requiring identifiable actors, attributable conduct, and established intent — encounter interpretative difficulties in anonymised environments that existing statutory provisions do not adequately address. Third, specific legislative gaps are identifiable in the IT Act, 2000 and the Bharatiya Nyaya Sanhita, 2023, particularly in relation to attribution of liability, effects-based jurisdiction, and evidentiary standards for digital records originating from encrypted networks. Fourth, enforcement limitations including constraints in forensic infrastructure, technical expertise, and international cooperation mechanisms suggest that legislative reform alone may be insufficient without corresponding institutional strengthening.

On the basis of this analysis, the study offers the following policy recommendations. First, targeted legislative amendments to the IT Act, 2000 may be considered to incorporate provisions specifically addressing anonymised network environments, including explicit attribution standards and an effects-based jurisdictional clause for cross-border cyber offences. Second, evidentiary frameworks under the Bharatiya Sakshya Adhiniyam, 2023 may benefit from procedural clarification regarding the admissibility of digital evidence collected from encrypted and anonymised sources, drawing on established judicial guidance in Anvar P.V. v. P.K. Basheer. Third, institutional capacity building within law enforcement agencies including the establishment of specialised cybercrime investigation units with dedicated dark web forensic capabilities may contribute meaningfully to more effective enforcement outcomes. Fourth, India may consider strengthening its bilateral legal cooperation framework through the negotiation of cybercrime-specific mutual assistance arrangements with key jurisdictions, to address the structural limitations of existing MLAT mechanisms.

The findings of this study carry several significant implications for legal scholarship, policy, and practice. For legal scholars, the study contributes a systematic doctrinal analysis of dark web-related legal challenges within the Indian framework an area that has received limited dedicated scholarly attention. For policymakers, the identification of specific legislative gaps in attribution, jurisdiction, and evidentiary standards provides a foundation for targeted reform initiatives. For enforcement agencies, the study underscores the need for institutional capacity building and specialised forensic infrastructure as necessary complements to legislative action. More broadly, the study contributes to the growing body of scholarship on cybercrime governance in the Global South, offering an India-specific analytical framework that may be of relevance to comparable jurisdictions navigating similar regulatory challenges.

It is acknowledged that this study is based exclusively on secondary sources and adopts a doctrinal methodology, which necessarily limits the scope of empirical engagement with enforcement realities. The reliance on publicly available legal texts and academic literature means that the practical dimensions of dark web enforcement — including investigative practices, prosecutorial strategies, and judicial decision-making remain beyond the scope of this analysis. Additionally, the rapidly evolving nature of dark web technologies means that legal frameworks and enforcement practices may require continuous adaptation, and findings presented here should be understood as reflective of the legal position at the time of writing. Future research may usefully extend this analysis through empirical investigation of law enforcement practices, judicial decision-making in cyber cases, and comparative analysis of regulatory frameworks across Global South jurisdictions facing similar challenges. Specific areas warranting further scholarly inquiry include: the constitutional dimensions of dark web regulation under the privacy framework established in K.S. Puttaswamy v. Union of India; the potential application of effects-based jurisdiction doctrines in Indian cyber law; the development of evidentiary standards specifically adapted to anonymised digital environments; and the scope for India's engagement with international cybercrime cooperation frameworks in a manner consistent with its data sovereignty concerns.

Abbreviations

BNS: Bharatiya Nyaya Sanhita, 2023, BSA: Bharatiya Sakshya Adhiniyam, 2023, IT Act: Information Technology Act, 2000, MLAT: Mutual Legal Assistance Treaty, UNODC: United Nations Office on Drugs and Crime.

Acknowledgement

The authors acknowledge the scholars, legal researchers, and judicial authorities whose published works on cyber law and cybercrime regulation have informed this study.

Author Contributions

Kriti Singh: Conceptualisation, Methodology, Investigation, Writing Original Draft, Writing Review and Editing, Gouri Malhotra: Writing — Review and Editing, Validation, Gaurav Kumar: Review and Editing.

Conflict of Interest

Kriti Singh declares no conflict of interest. Gouri Malhotra declares no conflict of interest. Gaurav Kumar declares no conflict of interest.

Data Availability

The data supporting the findings of this study are derived from publicly available secondary sources, including statutory provisions, judicial decisions, and academic literature. All relevant information is included within the article and cited references.

Declaration of Artificial Intelligence (AI) Assistance

The authors used AI Tools for language refinement and structural assistance, and Grammarly for grammar and formatting. The authors take full responsibility for the content, analysis, and integrity of the manuscript.

Ethics Approval

This study does not involve primary data collection from human participants or animals and is based entirely on secondary sources. Therefore, ethical approval and informed consent were not required. The study adheres to standard ethical guidelines for academic research and publication.

Funding

This research received no specific grant from any funding agency in the public, commercial, or not-for-profit sectors.

References

1. Hatta M. Deep web, dark web, dark net: A taxonomy of "hidden" internet. Ann Bus Adm Sci. 2020;19(6):277-92. doi:10.7880/abas.0200908a
2. Europol. Internet Organised Crime Threat Assessment (IOCTA) 2020. The Hague: Europol; 2020. https://www.europol.europa.eu/sites/default/files/documents/internet_organised_crime_threat_assessment_iocta_2020.pdf
3. Reddy S. Analytical study on cyber-crimes in India [Internet]. SSRN. 2021 Jun 15. https://dx.doi.org/10.2139/ssrn.4258578
4. Brenner SW. Cybercrime and the law: Challenges, issues, and outcomes. School of Law Faculty Publications. 2012;108. https://ecommons.udayton.edu/law_fac_pub/108/
5. Anvar P.V. v. P.K. Basheer. 2014. https://indiankanoon.org/doc/187283766/
6. Government of India. Bharatiya Nyaya Sanhita, 2023 (No. 45 of 2023). New Delhi: India Code; 2023. https://www.indiacode.nic.in/bitstream/123456789/20062/1/a202345.pdf
7. Government of India. Information Technology Act, 2000 (No. 21 of 2000). New Delhi: India Code. https://indiacode.nic.in/bitstream/123456789/131/1/it_act_2000_updated.pdf
8. Patil A. Navigating the digital landscape: India's evolving legal framework for e-commerce, data protection, and cybersecurity [Internet]. SSRN. 2024 May 29. doi:10.2139/ssrn.4850285
9. United Nations Office on Drugs and Crime (UNODC). Comprehensive study on cybercrime. Vienna: UNODC; 2013. https://www.unodc.org/documents/organized-crime/UNODC_CCPCJ_EG.4_2013/CYBERCRIME_STUDY_210213.pdf
10. Allison A. Role of international law in combating cross-border cybercrime: Addressing jurisdictional and enforcement challenges [Internet]. SSRN; 2025 Aug 12. doi:10.2139/ssrn.5806362
11. Convention on Cybercrime (Budapest Convention). European Treaty Series No. 185. Budapest: Council of Europe; 2001. https://rm.coe.int/1680081561
12. Shreya Singhal v. Union of India. 2015. https://indiankanoon.org/doc/110813550/
13. Avnish Bajaj v. State (NCT of Delhi). 2005. 3 CompLJ 364 Del (India). https://indiankanoon.org/doc/1308347/
14. K.S. Puttaswamy v. Union of India. 2017. https://indiankanoon.org/doc/91938676/
15. Bharati RK. Content regulation and stolen digital goods: Analysis of Sections 66A and 66B of the Information Technology Act, 2000 [Internet]. SSRN. 2025. doi:10.2139/ssrn.5378241
16. Singh M. Digital crimes and accountability gaps: A critical analysis of India's cyber law framework [Internet]. SSRN. 2026 Apr 20. doi:10.2139/ssrn.6395058
17. Chowbe VS, Chowbe TV. Cybercrime and the courts: Judicial insights in India and beyond. SSRN; 2025;11(4):228-35. doi:10.2139/ssrn.5001545
18. Sarkar G, Shukla SK. Policing transnational cybercrime: A critical assessment of the anticipated impact of the United Nations Convention against Cybercrime in India and worldwide [Internet]. SSRN. 2025;1-35. doi:10.2139/ssrn.5899223
19. Saxena V. Critical analysis of international cyber-crimes [Internet]. SSRN. 2023 Mar 14. doi:10.2139/ssrn.4383897
20. Government of India. Bharatiya Sakshya Adhiniyam, 2023. India Code. 2023. https://www.indiacode.nic.in
21. Bharati R, Khodke PG, Khadilkar CP, Bawiskar S. Forensic bytes: Admissibility and challenges of digital evidence in legal proceedings. Int J Sci Res Sci Technol. 2024;11(16):24-35. doi:10.2139/ssrn.4896874
22. Jain N. Admissibility of electronic evidence in India: An overview [Internet]. SSRN. 2021;1-18. https://dx.doi.org/10.2139/ssrn.3816724
23. Ganguli PA. Digital policing: Using social media surveillance to tackle cybercrime [Internet]. SSRN. 2025 Feb 5. doi:10.2139/ssrn.5124657
24. Meghwal T. Crime scene investigation in India: Legal framework, procedures and challenges [Internet]. SSRN. 2025 May 7. doi:10.2139/ssrn.5241244

25. Second Additional Protocol to the Convention on Cybercrime on Enhanced Co-operation and Disclosure of Electronic Evidence. European Treaty Series No. 224. Strasbourg: Council of Europe; 2022. https://www.wipo.int/wipolex/en/text/586521

How to Cite: Singh K, Malhotra G, Kumar G. Dark Web and Criminal Liability in India. Int Res J Multidiscip Scope. 2026; 7(3): 49-58. DOI: 10.47857/irjms.2026.v07i03.012119