# Jus Corpus Law Journal

Open Access Law Journal – Copyright © 2026 – ISSN 2582-7820

Editor-in-Chief – Prof. (Dr.) Rhishikesh Dave; Publisher – Ayush Pandey




# The Dark Web and Indian Cyber Law: A Need for Stricter Regulation


Srishti Keshri[a]

[a]Amity University, Jharkhand, India



*Received* 26 November 2025; *Accepted* 27 December 2025; *Published* 02 January 2026



*The anonymity capabilities, encryption tools, and decentralised nature offered by the dark web have proven to be the ideal haven for various forms of illegal activities, such as the smuggling of drugs, the sale of weapons, money fraud, identity theft, the distribution of child sexual content, and cyber terrorism. However, alongside the digital evolution of Indian society, encompassing the growth of e-governments, digital banking, and e-commerce, the susceptibility of individuals and organisations to such threats has inevitably escalated. Moreover, the present legislative system in the Indian context appears to struggle to effectively address the various complications arising from such advanced technologies and the functioning of the dark web. This paper critically evaluates the dark web and cyber laws applicable to India, specifically by considering existing provisions of the Information Technology Act 2000, along with penal sections of the Indian Penal Code, and constitutional frameworks. In essence, a doctrinal and analytical research is adopted to bring out deficiencies within the existing regimes concerning handling anonymous software, encryption-enabled communication, transactions via cryptocurrencies, and aspects of international jurisdictions. Decisions of superior courts, namely 'Shreya Singhal v Union of India' and 'Anvar P.V. v P.K. Basheer,' are discussed to interpret a balance between individual rights and state sovereignty. The paper establishes that, notwithstanding a robust cyber law structure, it still has imperfections to impact dark web-related crimes, which vividly establishes a need to tighten controls, promote intermediary liability, bolster cyber forensics, and promote international collaboration.*



**Keywords:** *dark web, Indian cyber law, information technology, cybercrime, intermediary liability.*

## INTRODUCTION

It is incredible how the internet is seen as a revolutionary tool to connect, trade, or share knowledge, yet it brought with it a lot of problems that are difficult to solve just by the laws or the governance. One of the most puzzling and frightening features of cyberspace is the dark web, a part of the internet that is not accessible with normal browsers and where new users who want to remain anonymous are allowed. Anonymity and encryption, while they may be the tools to preserve human rights and democracy in dictatorships, at the same time help an underground market where illegal activities flourish. The dark web is not only a complete playground for the traffickers of drugs and weapons, but it is also the place where they hijack the identity of others, exploit children, and even help terrorists to get money for their activities. Hence, it is one of the greatest dangers to world security and the safety of each country.

In India, where digitalisation has been going at a breakneck speed and has already brought significant changes in society and the economy, the dark web-associated risks are nothing but mild. The adoption of digital platforms for carrying out financial transactions, e-governance, and communication has, on the one hand, provided more opportunities to cybercriminals to carry out their illegal activities. On the other hand, the legal system in India, which mainly relies on the Information Technology Act, 2000 and is further supported by the Indian Penal Code, has been facing difficulties in adjusting to the new ways in which the criminals operate.[1] The problems of identification of the offender, figuring out which country's laws apply, and carrying out enforcement across borders make regulating the dark web even more difficult. Law courts have also been required to interpret the extent of existing laws, to stress the point of the necessity of law reforms and the need for greater clarification.

The purpose of this paper is to study the intersection of the dark web and Indian cyber law, both doctrinal and comparative, by examining legislative provisions, judicial trends, and enforcement mechanisms, as well as recognising the gaps that threaten the level of cyber resilience of the country. The research, by looking at India's response in the context of the world, is advocating for stricter regulation, technological innovation, and international cooperation as the essential strategies for fighting off the different dangers of the dark web.

[1] Information Technology Act 2000

The digital revolution is responsible for the changes in the lives of people, trade, ruling, and communication. However, this change also has some drawbacks. Besides the typical 'surface web' that is visible to search engines, and the 'deep web' that refers to non-indexed but legal databases (e.g., educational archives, health records), there is a 'dark web. Only through special tools such as Tor (The Onion Router), I2P, or Freenet can one enter the dark web, where it is possible to have completely anonymous dealings. Although anonymity is a great aid for whistleblowers and journalists under repressive regimes, it has also become a place for markets selling proscribed goods and for criminals' cyber activities to have platforms.

While the cybercrime incidents in India have sharply risen. National Crime Records Bureau (NCRB) Data shows that registered cybercrimes rose by over 200% from 2017 to 2022, with the majority of them comprising financial fraud, data theft, and the illegal online transaction of goods and services (NCRB, 2023).[2] Based on reports from law enforcement officials, it can be inferred that more than half of these illegal activities are associated with the dark web, either as stolen credit card dumps, drug sales, or hacking services.

## HISTORICAL DEVELOPMENT

Cyberlaws on a global scale emerged in the 1990s with the advent of e-commerce and hacking, but online also played a role in the introduction of cyberlaws. The very first of these laws mainly focused on issues related to unauthorised access to systems, data breaches, and digital contracts. The Information Technology Act, 2000, was the first legislation to regulate electronic transactions, provide for digital signatures, and deal with cyber offences in India.[3] The amendment in 2008 extended the coverage of the bill with the inclusion of identity theft, child pornography, cyber terrorism, and intermediary liability. However, the Act has always been a step behind the dark web marketplace and encrypted platform developments, most of the time, leading to some doctrinal loopholes in the regulation of anonymity, cryptocurrency transactions, and cross-border cybercrime.

[2] 'Cybercrimes Up 217% in the Past Five Years: Insights from the NCRB Report' (*Safer Internet India*, November 2025) <https://saferinternetindia.com/cybercrimes-up-217-in-the-past-five-years-insights-from-the-ncrb-report/> accessed 25 November 2025

[3] Information Technology Act 2000

## RELEVANCE TO PRESENT RESEARCH

This conceptual framework sets the dark web issue against the background of broader principles and philosophies of law. The Study references the principles of the rule of law, cyber sovereignty, deterrence, and privacy-security trade-off to assess how Indian cyber law might not only triumph over the existing challenge but also protect constitutional rights. It makes one ponder the areas of legislation, judicial interpretation, and enforcement where there may be chasms that, in turn, point out not only the necessity of having a system that can be both one that accepts the boundless digital space but also one that is conscious of privacy and basic human rights.

## IMPORTANCE OF THE STUDY

The dark web still threatens India, and its legal system challenges that keep arising and changing. Its very nature of the dark web - with all the secrecy and security features like encryption, decentralisation, and services that are not commonly known - makes it a real challenge for the agencies that enforce the law to catch criminals and bring them to justice. Furthermore, dark web crimes being transnational, i.e., crossing boundaries, weaken even more the effectiveness of traditional legal mechanisms that are based on territorial jurisdiction. As a result of these activities going so far beyond borders, workers dealing with people who sell drugs, smuggle weapons, exploit children, steal identities, commit financial fraud, or even finance terror, find themselves frightened by the concept and complexities of the whole issue and become absolutely reliant on international cooperation to be able to proceed with legal actions.

In India, the Information Technology Act 2000 (IT Act), supplemented by amendments, remains the mainstay in the fight against electronic crimes.[4] In addition to this, the Indian Penal Code (IPC),[5] the Indian Evidence Act 1872,[6] and the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021,[7] also contribute significantly to such a system. Although many in the field of law and research argue that this legislation, while being the backbone, is not enough to conquer the sophisticated, large-scale,

[4] *Ibid*
[5] Indian Penal Code 1860
[6] Indian Evidence Act 1872
[7] Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules 2021

and borderless nature of dark web crimes. There frequently exist struggles in the application of laws that manifest themselves as problems like the weakness of enforcement mechanisms, the lack of infrastructure for specialised cyber forensics, limited awareness by enforcement agencies, and insufficient synchronisation with international standards.

This research is important in a few ways. Firstly, the study profoundly uncovers the complicated connection between dark web activities and the legal and regulatory framework in India, differentiating those cases when the framework is advantageous from those when it is insufficient. Secondly, it also spots the doctrinal differences in the area of substantive and procedural laws and the enforcement gaps in the investigative and judicial processes. Thirdly, by opening up to comparisons of other countries such as the United States, the European Union, and other experts of cyberlaw, the study considers the coming of reforms in India that can be adapted to their socio-legal context. Finally, the research paper communicates a very urgent message about the need for a multi-strategic approach involving legislative reforms, technological innovations, undertaking capacity building, and international cooperation, and so being future-proof and comprehensive in their legal response.

## LITERATURE REVIEW

The Dark web is so clandestine a portion of the internet that there is no other way to access it other than through specific browsers such as Tor. It is likely best-known, perhaps, for whatever imaginable crime, including drug trade, cybercrime, kiddie porn, and terrorism. Weimann (2016) observes that because the dark web is anonymous, law enforcement officials are, irony of irony, prevented from effectively stamping down this content, which contrasts significantly with the more controlled surface web. In India, there is a debate about whether the current legal framework is adequate or needs to be tougher.

Most of this debate revolves around India's initial cyber law, the Information Technology Act 2000. The Act addresses numerous offences, some of which include hacking (Section 66), cyber terrorism (Section 66F), child pornography (Section 67B), and intermediary liability (Section 79).[8] It has been the criticism that the safe harbour provision under Section 79[9]

[8] Information Technology Act 2000, ss 66, 66F, 67B, and 79
[9] Information Technology Act 2000, s 79

implies that it limits the intermediaries to do as much as they can regarding the activities that relate to the dark web, even where they are implicated the most.

To back up the IT Act, the IPC[10] also came into action. Section 420 (concerning dishonesty), Section 468 (concerning the spread of malware), and Section 471 are used to address issues such as pseudonyms, documents, and banking scams related to the dark web.[11]

Section 65B of the Indian Evidence Act 1872[12] provides for the presentation before a court of electronic evidence.

India's Constitution also figures in the middle of the controversy. Article 19(1)(a)[13] treats free speech as a pledge, while Article 21[14] secures privacy. Article 19(2) allows reasonable restrictions for the sake of the interest of national security, the integrity of the country, and morals[15]. Briefly, the current research shows that although India does have some judicial proceedings against cybercrime, these are fragmented and outdated in nature. India's experience in expert laws, international cooperation, as well as cyber forensic laboratories, trails the U.S. and other EU countries. As most analysts conclude, something more effective is imminent as regards regulations, newer laws, and improved technological expertise to compare the rising threats of access to the dark web adequately.

## LEGISLATIVE PROVISIONS

**IT Act 2000:** The initial purpose of the IT Act 2000 was to create the legal framework for e-commerce, digital signatures, and to fix very basic cybercrime cases, such as unauthorised access and data leakage.

**2008 Amendment:** The areas of concern were broadened to include cyber terrorism, identity theft, child pornography, and intermediaries' liability. The scope was also accompanied by an increase in punishment and enforcement mechanisms.[16]

[10] Indian Penal Code 1860
[11] Indian Penal Code 1860, ss 420, 467, 471
[12] Indian Evidence Act 1872, s 65B
[13] Constitution of India 1950, art 19(1)
[14] *Ibid* art 21
[15] *Ibid* art 19(2)
[16] Information Technology (Amendment) Act 2008

**IT Rules, 2021:** The IT Rules, 2021, placed more demanding conditions on the intermediaries, for example, incoming content moderation, reporter details, and traceability of the source. Thus, the problem of accountability in the rapidly changing digital ecosystem has been resolved.[17]

**Section 66A (Struck Down in Shreya Singhal v Union of India 2015):** Section 66A was a legislation that described the case of a person who electronically communicated in an offensive, menacing, or false way.[18] Being ambiguously worded and thus open to misinterpretation, the law was used primarily to silence the dissenting voices of political opponents, social observers, and critics. In Shreya Singhal v Union of India (2015),[19] the Supreme Court of India declared the law unconstitutional based on freedom of speech under Article 19(1)(a)[20] violation and hence, voided it. Still, while no longer in place, those advocating for online speech control, even on anonymous forums like the dark web, cite the precedent set by this judgment.

**Section 69: Government Surveillance Powers:** Section 69 allows the government to access, supervise, or break into digital communication for the reasons of sovereignty, security, or public safety.[21] Although it is a crucial instrument in the fight against cybercriminals, the provision has been criticised for the absence of procedural safeguards and for the lack of disclosure. Provisions arouse the fear of potential exploitation and insufficient judicial supervision, particularly in cases of heavy encryption or on the dark web.

**Section 79: Safe Harbour for Intermediaries:** According to Section 79, intermediaries (such as Internet service providers, social media platforms) are not accountable for the content of third parties, provided that they undertake the necessary steps and, after receiving a notice, remove the content in question without fail.[22] The IT Rules, 2021, have more than doubled these responsibilities by requiring not only reactive content Moderation, but also the proactive traceability of originators.[23] These changes have a significant impact on the issue of the regulation of platforms or services that facilitate dark web transactions.

---

[17] Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules 2021
[18] Information Technology Act 2000
[19] *Shreya Singhal v Union of India* (2015) 5 SCC 1
[20] Constitution of India 1950, art 19(1)
[21] Information Technology Act 2000 , s 69
[22] Information Technology Act 2000, s 79
[23] Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules 2021

**Relevant Statutes and Constitutional Provisions —**

**Information Technology Act 2000 (IT Act):** The primary cyber law of India addressing cyber-attacks, theft of data, cyber terrorism, and child pornography is the Information Technology Act 2000. Besides this, it provides powers for interception and also regulates the liability of intermediaries. Still, it is quite old and not effective against the anonymity and international reach of the dark web.

- **Section 43:** Unauthorised access, data theft.
- **Section 66:** Hacking, identity theft.
- **Section 66F:** Cyber terrorism.
- **Section 67B:** Child pornography.
- **Section 69:** Power to intercept and monitor.
- **Section 79:** Intermediary liability.

**Indian Penal Code (IPC), 1860 —**

The code applies to various kinds of cheating, fraud, and forgery that are quite common on the dark web. Some provisions in the code can help in the prosecution of scammers and counterfeit documents that are being traded online. Nevertheless, as the code was written before the digital era, it still lacks the necessary elements of clarity for the complicated cybercrimes.

- **Section 420:** Cheating and fraud.
- **Section 468:** Forgery for cheating.
- **Section 471:** Using forged electronic documents.

**Indian Evidence Act 1872 —**

This act acknowledges electronic evidence during court hearings as per Section 65B. The dark web data is most of the time encrypted or volatile; hence, complying with the law is quite difficult. So, the rules of evidence need to be converted for cybercrime cases.

**Section 65B:** Admissibility of electronic evidence.

**Constitution of India —**

It offers the right to speech (Article 19(1)(a)) and the right to privacy (Article 21). The reasonable restrictions (Art 19(2)) give security and morality grounds to restrict free speech. Therefore, the rights must be weighed against the danger of dark web abuse.

- **Article 19(1)(a):** Freedom of Speech.
- **Article 19(2):** Reasonable Restrictions.
- **Article 21:** Right to Privacy.

**CONCEPTUAL FRAMEWORK DOCTRINES**

**Rule of Law:** Basically, the rule of law concept is a very simple idea, yet very powerful, that law enforcement agencies must follow certain legal standards, which will also set out what constitutes a crime in the cyberspace domain. The way the laws are explained also separates the legal and illegal usage of the anonymity tools; thus, on the one hand, it reduces the chance of the arbitrary application of the law and, on the other hand, it ensures that the citizens' basic rights are not violated.

**Cyber Sovereignty:** Cyber sovereignty is the concept that indicates that they have the power over those things that happen in the cyber world within their geographical boundaries. As the dark web crimes are mostly cross-border, this principle poses very complicated questions of jurisdictional areas, cross-border investigation, and international collaboration. The principle forms the basis of India's legal framework to enable the court to exercise jurisdiction over cybercrimes that threaten national security or Indian citizens, regardless of whether the offenders are from India or not.

**Deterrence Theory:** The deterrence theory states that the reason for low crime is the putting in place of stricter laws, having very well-defined penalties and efficient enforcement. While

Talking about the dark web, this concept not only demonstrates the need for strict laws but also emphasises the requirement of having an able law enforcement to discourage the criminals from using such encrypted and anonymous spaces.

**Privacy v Security:** This issue is one of the most important problems raised by the regulation of the encrypted platforms. The dark web gives users the possibility to remain anonymous

and keep their privacy, while at the same time, it gives criminals a place where they can operate without being detected. Privacy fighting against state security is still present in the sphere of law and policy within the context of cybercrime, and is basically connected with Article 21.

## JUDICIAL ANALYSIS

**Shreya Singhal v Union of India (2015):** This was one of the landmark cases where the Supreme Court of India unequivocally struck down Section 66A of the IT Act, 2000, which prohibited sending of offensive, scary, or false messages through the net.[24] The Court found the provision lacking in clarity, too broad in scope, and also at odds with Article 19(1)(a) (freedom of speech and expression).[25] Through its verdict, the Court emphasised that criminalising online speech without laying down exact standards for what can be prosecuted might lead to repression of political dissent, criticism, and possible other forms of expression. The case is a lot like many others that show the law courts protecting the fundamental human rights while simultaneously acknowledging the state's safety concerns and fostering the requirement of clear legal definitions for regulating online speech, especially when anonymity is preserved by the dark web.[26]

**Anvar P.V. v P.K. Basheer (2014):** If we talk about the Supreme Court, it is a case in which the highest judiciary has established its viewpoint on the required proof standard for electronic records in Section 65B of the Indian Evidence Act, 1872.[27] The Court decides that all those secretions mentioned in Section 65B should be complied with for electronic evidence to be admitted, among which is the certification by the person in charge of the electronic record.

Appliances with this verdict have a strong impact on the dark web cases, where data is typically in the form of encrypted communications, transaction logs, or digital

[24] Information Technology Act 2000, s 66A
[25] 'Freedom of Speech & Expression' (*Drishti Judiciary*, 20 November 2023) <https://www.drishtijudiciary.com/to-the-point/ttp-constitution-of-india/freedom-of-speech-%26-expression> accessed 25 November 2025
[26] *Shreya Singhal v Union of India* (2015) 5 SCC 1
[27] Indian Evidence Act 1872, s 65B

communications. Proper following of Section 65B makes it so that the electronic evidence from the dark web is legally valid and is capable of passing judicial inspections.[28]

**BARRIERS**

Regulation of the dark web in India faces various challenges that make regulation and law enforcement ineffective. One significant challenge is the technology used on the dark web. Use of advanced encryption, blockchain payment, and anonymisation tools such as Tor and VPN makes it extremely difficult for law enforcers to track actors. Even when a criminal activity is proven, tracing it back becomes very difficult, thus leaving loopholes for criminals to escape punishment.

Secondly, there is a legal barrier due to the constraints of the cyber laws in India. The Information Technology Act 2000 in India is archaic in several aspects since it was not initially made to deal with anonymous globalised crime. The provisions of the Indian Penal Code are also not adequately addressing cross-border cybercrimes, therefore leaving gigantic loopholes in the law. Further, safe harbour and intermediary liability issues are hindering the potential of platforms and service providers in effectively preventing dark web-related crimes.

Structural problems also add to the problem. India does not have adequate cyber forensic laboratories, trained staff, and cross-border coordination mechanisms. While Western countries such as the U.S. and EU countries are spending heavily on specialist forces, India's law enforcement is usually underfinanced and overworked. Jurisdictional challenges also abound because most dark web servers and operators are beyond the territorial jurisdiction of India, and hence international coordination becomes a necessity, but more often than not, a challenge.

Lastly, there are constitutional and societal barriers. The conflict between surveillance, civil liberties, and privacy is still contentious. Bureaucratizing surveillance could go against constitutional safeguards under Articles 19 and 21.[29] This has stalled legislative reforms, otherwise potentially enhancing regulatory power. In sum, the four-pronged challenges for

[28] *Anvar P V v P K Basheer & Ors* (2014) 10 SCC 473
[29] 'Right to Freedom (Articles 19–22)' *(BYJU'S)* <https://byjus.com/free-ias-prep/right-to-freedom-articles-19-22/> accessed 25 November 2025

India are technological, legal, institutional, and constitutional, thus cumulatively contributing to a regulatory gap to be exploited by dark web actors.

**PROGRESS ACHIEVED**

In spite of all these impediments, India has registered good progress in dealing with cybercrime and dark web–based crimes. The Information Technology Act, 2000, however old, offers a basic framework that has been augmented by amendments, judicial pronouncements, and supporting legislation. Cyber terrorism, for example, is criminalised by Section 66F, while Section 67B deals with child pornography—both being prevalent crimes on the dark web.

Also, Indian courts have increasingly appreciated the probative value of digital records. The Indian Evidence Act has provided for the admissibility of electronic evidence in trials through Section 65B, establishing a procedural mechanism for prosecuting cybercrimes. This is an improvement towards ensuring that digital traces, even if incomplete, can be put before the courts.

On the enforcement side, India has created specialised cybercrime cells in large cities, and the National Critical Information Infrastructure Protection Centre (NCIIPC) also contributes to protecting sensitive infrastructure. The creation of the Indian Cyber Crime Coordination Centre (I4C) also marks a structural response to increasing cyber threats, including those that originate from the dark web.

India has also become part of international efforts at cybercrime collaboration. Participation in INTERPOL's programs on cybercrime and bilateral arrangements with nations such as the U.S. enable Indian agencies to exchange intelligence and technical know-how. Additionally, training schemes for law enforcement personnel have enhanced their knowledge of cyber threats and the equipment necessary to uncover them.

At a policy level, initiatives concerning data protection legislation and digital sovereignty reflect the acknowledgement by India of the imperative to update its cyber governance matrix. Even as these initiatives are ongoing, they cumulatively point to a direction of incremental enhancement. Accordingly, even though India's initiatives are still disjointed, the gains made reflect a desire to improve its cyber resilience to dark web threats.

## PROGRESS ACHIEVED

In spite of all these impediments, India has registered good progress in dealing with cybercrime and dark web–based crimes. The Information Technology Act, 2000, however old, offers a basic framework that has been augmented by amendments, judicial pronouncements, and supporting legislation. Cyber terrorism, for example, is criminalised by Section 66F, while Section 67B deals with child pornography—both being prevalent crimes on the dark web.

Also, Indian courts have increasingly appreciated the probative value of digital records. The Indian Evidence Act has provided for the admissibility of electronic evidence in trials through Section 65B, establishing a procedural mechanism for prosecuting cybercrimes. This is an improvement towards ensuring that digital traces, even if incomplete, can be put before the courts.

On the enforcement side, India has created specialised cybercrime cells in large cities, and the National Critical Information Infrastructure Protection Centre (NCIIPC) also contributes to protecting sensitive infrastructure. The creation of the Indian Cyber Crime Coordination Centre (I4C) also marks a structural response to increasing cyber threats, including those that originate from the dark web.

India has also become part of international efforts at cybercrime collaboration. Participation in INTERPOL's programs on cybercrime and bilateral arrangements with nations such as the U.S. enable Indian agencies to exchange intelligence and technical know-how. Additionally, training schemes for law enforcement personnel have enhanced their knowledge of cyber threats and the equipment necessary to uncover them.

At a policy level, initiatives concerning data protection legislation and digital sovereignty reflect the acknowledgement by India of the imperative to update its cyber governance matrix. Even as these initiatives are ongoing, they cumulatively point to a direction of incremental enhancement. Accordingly, even though India's initiatives are still disjointed, the gains made reflect a desire to improve its cyber resilience to dark web threats.

## CONCLUSION

The emergence of dark web-facilitated crimes has become a great menace not only for India but also for the whole world. On a global level, the dark web has been the main medium for the transportation of illegal drugs, arms, and identities, as well as for the exploitation of children and cyberterrorism. India, being a digital country of the world that is slowly moving towards e-commerce, must be aware that it also faces threats of this nature. Although the IT Act, 2000, is primarily a legal framework for India, it is still considered to be largely inadequate to deal with the technological complexity of the dark web, such as anonymity tools, cryptocurrencies, and encrypted marketplaces.

Judicial interventions, for instance, the case of Shreya Singhal v Union of India and Anvar P.V. v P.K. Basheer, are a demonstration of the commitment towards constitutional rights protection and the assurance of due process. Despite that, courts alone cannot take on dark web criminals. They need more help from the legislature in terms of manpower for enforcement and the cooperation of other countries in this matter. The comparative study of jurisdictions such as the United States and the European Union reveals that India is behind in the areas of technical enforcement and formal participation in global cybercrime treaties; thus, there exist gaps in effective cross-border investigation and prosecution.

Overhaul the IT Act to include clear provisions that describe darknet marketplaces, cryptographic currencies, and anonymising technologies.

Besides that, you can solve the issue of intermediary accountability by the introduction of safeguards related to procedural fairness that will guarantee that the content disclosure will be done in a responsible way and at the same time will not violate the freedom of expression of the users. Create cybercrime units in every state, make sure that the employees are properly trained, and install forensic labs. A group of professionals can be trained in blockchain forensics, Tor data traffic analysis, and given AI-based threat alert systems to guide them.