INTERNATIONAL JOURNAL OF HUMAN RIGHTS LAW REVIEW

Volume 4 | Issue 1 Art. 9

2025

Navigating the Challenges in Creating a Legal Framework for Dark Web Regulation

Ayesha Khanum and Jyotirmoy Banerjee

Recommended Citation
Ayesha Khanum and Jyotirmoy Banerjee, *Navigating the Challenges in Creating a Legal Framework for Dark Web Regulation*, 4 IJHRLR 114-125 (2025).
Available at www.humanrightlawreview.in/archives/.

Navigating the Challenges in Creating a Legal Framework for Dark Web Regulation

Ayesha Khanum and Jyotirmoy Banerjee

LLM Student, Amity Law School, Amity University, Bengaluru
Assistant Professor, Amity Law School, Amity University, Bengaluru

Manuscript Received	Manuscript Accepted	Manuscript Published
04 Jan. 2025	06 Jan. 2025	08 Jan. 2025

ABSTRACT

The dark web is a segment of the internet that provides anonymity to its users, presents significant regulatory challenges due to its decentralized nature and its dual role in facilitating both legitimate and illicit activities. While it serves as a platform for privacy-conscious individuals, such as journalists and activists, the dark web has also become a hub for cybercrime, trafficking, and other illegal activities. This article explores the key challenges faced in creating an effective legal framework for dark web regulation. It focuses on jurisdictional issues, the balancing of privacy with security, and technological obstacles. The anonymity provided by technologies like Tor and encryption tools makes it difficult for law enforcement to trace illegal activities, creating a complex legal landscape that transcends national borders. The lack of a unified international regulatory approach further complicates efforts to tackle cybercrime on the dark web. Additionally, the need to protect users' privacy while preventing criminal activities raises ethical concerns about the potential overreach of surveillance and the erosion of civil liberties. The article analyses current regulatory attempts and underscores the importance of international cooperation, technological innovation, and clear legal frameworks to address the challenges effectively. It also discusses the ethical implications of regulating the dark web, particularly the need to safeguard fundamental rights such as free speech and privacy. The article concludes with recommendations for enhanced global collaboration, investment in new technologies, and the establishment of legal precedents that balance privacy with security. Ultimately, the regulation of the dark web requires a careful, adaptable

approach that ensures both the safety of the digital environment and the protection of individuals' rights in an increasingly interconnected world.

KEYWORDS

Dark Web, Cybercrimes, Tor, Privacy, Dark Web.

INTRODUCTION

The dark web is a hidden segment of the internet that is not indexed by standard search engines and requires specific tools or configurations to access. It forms part of the "deep web," which encompasses all content not accessible through conventional search engines, such as private databases, intranet systems, and paywalled websites. Unlike the deep web, the dark web is intentionally concealed and designed to provide anonymity for its users, which has made it both a haven for privacy-conscious individuals and a hub for illicit activities.

Accessing the dark web typically involves using specialized software, such as The Onion Router (Tor) or Invisible Internet Project (I2P). These tools mask users' IP addresses and encrypt data, creating a layer of anonymity. Tor, the most commonly used tool, routes internet traffic through a network of volunteer-operated servers, effectively obscuring a user's identity and location. Similarly, I2P creates encrypted peer-to-peer communication channels, facilitating anonymous browsing and hosting of services.[1]

The dark web operates using decentralized, encrypted networks known as "darknets." Websites hosted on the dark web use special domain extensions, such as "onion" for Tor, which are inaccessible through standard web browsers without the corresponding software. Services hosted on the dark web include marketplaces, forums, communication platforms, and hidden websites, all of which rely on anonymity as a core feature. These sites are often transient, appearing and disappearing without notice, further complicating their regulation and oversight.[2]

While the dark web serves legitimate purposes, such as protecting whistleblowers, enabling freedom of speech in oppressive regimes, and securing communications for journalists and activists, it is also used for illegal activities. These include the trade of drugs, weapons, counterfeit documents, and hacking services, as well as hosting platforms for cybercrime, human

[1] Ahmed Ghappour, *Searching Places Unknown: Law Enforcement Jurisdiction on the Dark Web*, 69 Stan. L. Rev. 1075 (2017).
[2] Ibid.

trafficking, and extremist content. The dark web's dual-use nature makes it a unique and complex phenomenon, necessitating a nuanced approach to its regulation and governance.

CHALLENGES IN REGULATING THE DARK WEB

- ***Jurisdictional and International Issues***

The dark web's decentralized and global nature complicates the enforcement of territorial laws, as criminals can operate across borders, with servers hosted in jurisdictions that may lack robust cybercrime legislation. This borderless environment demands international cooperation, yet conflicting legal frameworks across countries exacerbate the problem.[3] While some nations criminalize dark web usage for illicit purposes, others lack specific regulations or prioritize privacy over surveillance, creating safe havens for cybercriminals.[4] For instance, the uneven adoption of the Budapest Convention on Cybercrime reflects these disparities, with several major countries remaining outside its purview. Enforcement efforts are further hindered by technical barriers, such as encryption tools like Tor, resource gaps in developing nations, and coordination challenges among law enforcement agencies with differing priorities. High-profile operations like the takedown of Silk Road and Europol's "Dark HunTor" demonstrate the necessity of cross-border collaboration but also reveal the logistical and ethical difficulties involved. Additionally, ethical concerns arise in balancing security with privacy, as surveillance technologies employed to track dark web activities risk infringing on civil liberties.[5]

To address these challenges, a unified global framework is essential, fostering harmonized laws, information sharing, and ethical enforcement mechanisms. International treaties like the Budapest Convention must be expanded and adapted to address the complexities of dark web regulation, ensuring a balance between combating cybercrime and protecting individual rights. Ultimately, effective dark web governance requires a proactive, collaborative global approach that transcends jurisdictional boundaries.

[3] George Caleb Oguta, *Securing the Virtual Marketplace: Navigating the Landscape of Security and Privacy Challenges in E-Commerce*, 18 GSC Advanced Research and Reviews 084 (2024)/
[4] Ibid.
[5] Mohsin Dhali et al., *Cryptocurrency in the Darknet: Sustainability of the Current National Legislation*, 65 International Journal of Law and Management 261 (2023).

- ***Balancing Privacy and Security***

At the heart of dark web regulation lies the challenge of balancing privacy and security. The very technologies that protect anonymity—such as Tor (The Onion Router) and end-to-end encryption—are also the same technologies that enable criminal activities. On the one hand, privacy protections are essential for users concerned about surveillance, oppression, or censorship. On the other hand, the same anonymity tools can provide cover for criminal networks.[6] Striking the right balance between protecting individuals' right to privacy and enabling law enforcement agencies to investigate and prosecute illicit activities is crucial. Any regulation or intervention must consider the risks of overreach, which could lead to mass surveillance and infringements on fundamental rights.

- ***Technological Challenges***

Technology is both a boon and a barrier to effective regulation. The decentralized and encrypted nature of the dark web makes it difficult for law enforcement agencies to track criminal activities, such as drug trafficking or money laundering.[7] While various technological tools and techniques, such as blockchain analysis or AI-powered surveillance, have been developed to detect and prevent illegal activities, the rapid evolution of technologies used by dark web users often outpaces regulatory efforts. For example, once one method of tracking dark web activity is implemented, new tools or networks are quickly created to evade detection. The constant technological arms race between regulators and cybercriminals is one of the defining challenges in dark web governance.[8]

LEGAL FRAMEWORKS FOR REGULATING THE DARK WEB IN INTERNATIONAL CONTEXT

Regulating the dark web at an international level requires

[6] Shinu Vig, Sunita Dwivedi, & Reenu, *Navigating the Ethical, Social and Legal Implications of Metaverse*, *in* 2024 15th International Conference on Computing Communication and Networking Technologies (ICCCNT) 1 (2024), https://ieeexplore.ieee.org/abstract/document/10724741 (last visited Dec 30, 2024).

[7] Saiba Nazah et al., *Evolution of Dark Web Threat Analysis and Detection: A Systematic Approach*, 8 IEEE Access 171796 (2020), https://ieeexplore.ieee.org/abstract/document/9197590 (last visited Dec 30, 2024).

[8] Taking on the Dark Web: Law Enforcement Experts ID Investigative Needs | National Institute of Justice, https://nij.ojp.gov/topics/articles/taking-dark-web-law-enforcement-experts-id-investigative-needs (last visited Dec 30, 2024).

cohesive legal frameworks that address its borderless and decentralized nature while promoting collaboration among nations.[9] Currently, international efforts to govern the dark web are fragmented, with significant reliance on existing treaties, regional agreements, and cooperative mechanisms. Some of the key legal frameworks and approaches aimed at addressing the challenges of regulating the dark web globally-

- ***Budapest Convention on Cybercrime (2001)***

The Budapest Convention on Cybercrime is the first and most comprehensive international treaty addressing cybercrime, including crimes facilitated by the dark web. It provides a framework for harmonizing national laws, fostering international cooperation, and enhancing investigative capabilities. The treaty outlines mechanisms for handling transnational cybercrime, such as data-sharing agreements, expedited preservation of stored data, and mutual legal assistance. It establishes clear guidelines for international collaboration and sets a standard for member countries to follow.[10]

- ***United Nations Resolutions and Initiatives***

The United Nations (UN) has adopted various resolutions to combat cybercrime and regulate the misuse of technologies, including those used on the dark web. Resolution 75/282 on Countering the Use of the Internet for Criminal Purposes emphasizes international cooperation to address dark web crimes like human trafficking, drug trafficking, and terrorism. The United Nations Office on Drugs and Crime (UNODC) has also played a pivotal role by providing technical assistance and capacity-building for countries to tackle cybercrime, including dark web-related offenses.

- ***Regional Agreements***

Regional organizations have developed frameworks to address dark web-related crimes, often tailored to specific geopolitical challenges. The European Union (EU) The EU's Cybersecurity Strategy and Directive on Security of Network and Information Systems (NIS Directive) provide guidelines for member states

[9] Weiwei Yi & Zihao Li, *Mapping the Scholarship of Dark Pattern Regulation: A Systematic Review of Concepts, Regulatory Paradigms, and Solutions from an Interdisciplinary Perspective*, (2024), http://arxiv.org/abs/2407.10340 (last visited Dec 30, 2024).

[10] Mario Lopez, *Global Digital Governance: Navigating the Future of a Connected World*, (2024), https://papers.ssrn.com/abstract=4995445 (last visited Dec 30, 2024).

to improve cybersecurity and cooperate on investigating dark web crimes. Europol's European Cybercrime Centre (EC3) coordinates cross-border investigations into dark web marketplaces.[11] The Malabo Convention on Cybersecurity and Personal Data Protection aims to address cybercrime and data protection but faces challenges in implementation due to limited resources in many member states. Bilateral and multilateral MLATs enable countries to request legal assistance from one another in investigating and prosecuting crimes involving the dark web. These treaties facilitate the sharing of evidence, extradition of suspects, and cooperation in dismantling criminal networks. It provides a structured process for cross-border collaboration.

- ***Global Law Enforcement Initiatives***

International organizations like Interpol and Europol have established frameworks for tackling cybercrime and dark web offenses. Interpol's Global Cybercrime Programme provides a platform for intelligence-sharing and capacity-building among member states. Europol's operations, such as "Dark HunTor," demonstrate the importance of international task forces in targeting illegal activities on the dark web. But the lack of a uniform legal framework for regulating the dark web further complicates the issue. Different countries have developed varying approaches, ranging from attempts to monitor or shut down dark web access to focusing on specific illicit activities.[12] Some countries, such as the United States, have focused on criminalizing access to the dark web for certain illegal activities, while others may be more permissive. Moreover, legal frameworks must contend with ethical issues, such as ensuring that regulation does not infringe upon freedom of speech, privacy rights, or access to information. Furthermore, the ethical dilemma of censoring content that may be harmful but also may include valuable information for activism or research complicates the regulatory approach.

LEGAL FRAMEWORK REGULATING THE DARK WEB IN INDIA

- ***Information Technology Act, 2000 (IT Act)***

The IT Act, 2000, is India's primary legislation governing cyber activities. Although it does not explicitly mention the dark web, several provisions are relevant:

[11] Ahmed Ghappour, *Searching Places Unknown: Law Enforcement Jurisdiction on the Dark Web*, 69 Stan. L. Rev. 1075 (2017).
[12] Michael Chertoff, *A Public Policy Perspective of the Dark Web*, 2 Journal of Cyber Policy 26 (2017).

- **Section 66**: Penalizes hacking, identity theft, and related offenses often linked to dark web activities.

- **Section 67**: Prohibits publishing or transmitting obscene material online, addressing content frequently circulated on dark web platforms.

- **Section 69**: Empowers the government to intercept, monitor, and decrypt information in the interest of national security. This includes tracking dark web activities where feasible.

- **Section 79**: Provides intermediary liability protections but mandates intermediaries (like internet service providers) to remove unlawful content when notified.[13]

- ***Bharatiya Nyaya Sanhita, 2023***

The Bharatiya Nyaya Sanhita (BNS), 2023, which replaces the Indian Penal Code, 1860, includes provisions that can address crimes facilitated via the dark web, such as drug trafficking, cyberstalking, and online harassment. These provisions correspond to earlier sections of the IPC and are relevant in combating offenses originating on the dark web:

1. **Sections 302 to 308**: Address extortion and blackmail, including crimes akin to ransomware attacks facilitated through the dark web.

2. **Section 316**: Deals with cheating and fraud, which are commonly associated with financial scams conducted on dark web platforms.

3. **Section 109**: Covers criminal conspiracy, targeting organized crime networks operating via dark web marketplaces.[14]

- ***Narcotic Drugs and Psychotropic Substances Act, 1985 (NDPS Act)***

India's NDPS Act is particularly relevant to the dark web, as online marketplaces like Silk Road have been used to facilitate the trafficking of illegal drugs. The Act's provisions empower law enforcement agencies to monitor and prosecute drug-related offenses, including those committed via the dark web.[15]

[13] Information Technology Act, 2000 (IT Act)
[14] Bharatiya Nyaya Sanhita, 2023
[15] Narcotic Drugs and Psychotropic Substances Act, 1985 (NDPS Act)

Cryptocurrency Regulations

Cryptocurrencies, often used for transactions on the dark web, are not fully regulated in India. However, recent developments indicate a move toward regulation:

- The Cryptocurrency and Regulation of Official Digital Currency Bill, 2021, aims to address the use of cryptocurrencies, including their potential misuse on the dark web.
- The Prevention of Money Laundering Act, 2002 (PMLA), applies to cryptocurrency transactions, aiming to curb money laundering and terror financing linked to dark web activities.

CERT-In Guidelines

The Indian Computer Emergency Response Team (CERT-In) is a key agency for addressing cyber threats in India. It issues advisories and monitors cybercrimes, including those originating from the dark web. The recent CERT-In Directions of 2022 mandate reporting of cyber incidents within six hours, potentially aiding in the identification of dark web-related activities.

CHALLENGES IN IMPLEMENTING LEGAL FRAMEWORKS IN DARK WEB

Implementing regulations for the dark web faces significant limitations due to its inherently anonymous and decentralized nature. One of the primary challenges is the technical complexity of the dark web, which operates using advanced encryption technologies and decentralized networks, making it difficult for law enforcement agencies to trace users or monitor activities effectively.[16] Tools like Tor and I2P obscure user identities and locations, complicating surveillance and investigation efforts. Jurisdictional issues further hinder enforcement, as the borderless nature of the dark web allows criminal activities to span multiple countries, each with its own legal frameworks and priorities.[17]

[16] Shubha Ojha, *Surge in Dark Web Crimes, the Indian Legal Scenario and 'International Cooperation' as the Way Forward*, *in* Proceedings of the 17th International RAIS Conference on Social Sciences and Humanities 131 (0), https://www.ceeol.com/search/chapter-detail?id=885777 (last visited Dec 30, 2024).

[17] Sara Bardhant & Pallabhi Chakraborty, *The Dark Web's Influence on International Relations: Unravelling the Hidden Threads*, 2 Journal of Judikaltura 1 (2024).

Disparities in cybercrime laws and the lack of universal adoption of treaties like the Budapest Convention exacerbate this challenge, creating safe havens for cybercriminals in jurisdictions with weak regulations. Additionally, resource constraints, particularly in developing nations, limit the ability to invest in advanced technologies and trained personnel required to combat dark web crimes. Ethical concerns also arise, as intrusive surveillance measures to regulate the dark web risk infringing on privacy rights and civil liberties, potentially leading to public backlash. These limitations highlight the need for international cooperation, robust technological solutions, and a balanced approach to ensure effective regulation while safeguarding individual freedoms.

THE FUTURE OF DARK WEB REGULATION

As the dark web continues to evolve, so too must the legal frameworks that govern it. There are several possible directions for the future of regulation:

1. Given the global nature of the dark web, it is imperative that countries work together to create multilateral agreements to combat cybercrime and regulate illicit activities.[18] Information-sharing agreements, harmonizing laws related to cybercrime, and coordinated law enforcement efforts could lead to a more effective global response.

2. Regulators must invest in new technologies to track and prevent criminal activity on the dark web. AI, machine learning, and data analytics can help identify illegal activities without violating users' privacy rights. However, the technological tools used by both law enforcement and dark web users need to be constantly updated to stay ahead of cybercriminals.[19]

3. Any regulation must carefully define the boundaries between legitimate and illegitimate activity. Legal frameworks should focus on clearly defined criminal activities while respecting fundamental rights such as free speech and privacy. Oversight mechanisms should be put

[18] Ulrich Gasper, *Ethical and Societal Issues of Automated Dark Web Investigation: Part 5*, *in* Dark Web Investigation 189 (Babak Akhgar et al. eds., 2021), https://doi.org/10.1007/978-3-030-55343-2_10 (last visited Dec 30, 2024).
[19] Philip J. Weiser, *The Future of Internet Regulation*, 43 U.C. Davis L. Rev. 529 (2009).

in place to prevent potential abuses of power and ensure that regulation does not encroach on personal freedoms.[20]

4. Governments should also invest in educating citizens about the risks of the dark web and how to protect themselves from cybercrimes. Public awareness campaigns could help reduce the number of individuals inadvertently engaging in illegal activities on the dark web.[21]

CONCLUSION

The dark web poses a distinct challenge in the creation of legal frameworks due to its inherently anonymous and decentralized nature. Striking a balance between ensuring security and preserving the principles of privacy and freedom is critical, as over-regulation risks infringing on fundamental human rights. While the dark web enables illicit activities such as drug trafficking, cybercrime, and human exploitation, it also serves as a vital resource for whistleblowers, journalists, and individuals seeking to evade censorship in oppressive regimes. Thus, any regulatory framework must carefully navigate these dualities, ensuring that legitimate uses of the dark web are protected while combating illegal activities effectively.

International cooperation is indispensable in addressing dark web crimes, given their transnational nature. Criminal networks operating on the dark web often span multiple jurisdictions, exploiting inconsistencies in national laws. Collaborative efforts, such as those facilitated by the Budapest Convention on Cybercrime, can enhance intelligence sharing, streamline evidence collection, and foster coordinated enforcement actions across borders. However, many countries remain outside such frameworks, necessitating new agreements that are inclusive and reflective of diverse legal systems.[22]

Technological innovation is another cornerstone of dark web regulation. Law enforcement agencies need advanced tools, such as AI-driven analytics and blockchain tracing systems, to monitor and disrupt illicit activities. Simultaneously, these tools

[20] Robert W Gehl, *Power/Freedom on the Dark Web: A Digital Ethnography of the Dark Web Social Network*, 18 New Media & Society 1219 (2016).
[21] Vincent Harinam & Barak Ariel, *The Role of Law Enforcement in the Regulation of Cryptomarkets (and the Limited Role of Deterrence)*, *in* Law Enforcement Strategies for Disrupting Cryptomarkets: A Practical Guide to Network Structure, Trust Dynamics, and Agent-Based Modelling Approaches 49 (Vincent Harinam & Barak Ariel eds., 2024), https://doi.org/10.1007/978-3-031-62821-4_3 (last visited Dec 30, 2024).
[22] Lawrence J. Trautman, *Virtual Currencies; Bitcoin & What Now after Liberty Reserve, Silk Road, and Mt. Gox?*, (2014), https://papers.ssrn.com/abstract=2393537 (last visited Dec 30, 2024).

must be deployed with strict oversight to prevent abuse and ensure compliance with privacy standards. Establishing clear legal precedents is essential to define the scope of permissible actions for both governments and private entities, providing clarity on issues like surveillance, data collection, and encryption.

Finally, an adaptive legal approach is crucial to keep pace with the rapidly evolving nature of internet and dark web technologies. Legislative frameworks must be forward-thinking, anticipating future developments while addressing current threats. By combining global collaboration, ethical considerations, and carefully crafted legislation, societies can work toward creating a secure online ecosystem that upholds the principles of freedom, privacy, and justice.