Dark Web as Nexus for Money Laundering and Environmental Crimes: An Analytical Study on Legal Challenges and Enforcement Strategies

Mr Rushi Bhagat[1]
Dr Jiya Mathrani[2]

Abstract

This article focuses on the role of the Dark Web, which facilitates Environmental crimes and Money Laundering, emphasising the nexus between illicit activities and managing illicit proceeds, despite having legislative frameworks and a jurisdictional landscape. There is a lack of technical capacity and India's inability to combat money laundering and environmental crimes through the dark web. The dark web provides a platform for Environmental crime perpetrators to operate anonymously in the Illicit trade of products obtained through Illegal logging and Mining; hence, this incognito identity aids them in laundering the illicit proceeds. The study thoroughly analyses the Dark Web, examining its intersection with Environmental crimes and money laundering to inform legal precedents for updating the legal framework. This analysis examines the potential for collaboration between law enforcement agencies and environmental governance to address crime. The shift from conventional methods to the dark web is minimal, but it allows criminals to convert Illicit gains into cryptocurrencies and other forms of currency. Doctrinal research methodology is used to analyse laws, regulations and International Conventions to determine the country's efforts towards this goal. Also due to the complex nature of the dark web, the challenges faced by law enforcement agencies are examined by analysing the complex issues of the need for centralised national cooperation, international and national cooperation, and regulations of virtual assets like cryptocurrencies and robust mechanisms to dislocate the criminal network, fixing the jurisdictional barriers that deter the effective implementation of National-International mechanisms to curb Environmental crimes and money laundering, thus protect the environment dismantle the role of dark web in financial and environmental offences.

Key Words- *Environmental Crimes, Money Laundering, Dark Web, Legal framework, jurisdiction.*

[1] Research Scholar, GLS University, 9408754758, rushi.bhagat@glsuniversity.ac.in
[2] Assistant Professor, GLS University, Faculty of Law

Introduction

"Corruption undermines regulation and enforcement while technology accelerates the capacity of traffickers to reach global markets—criminal justice responses should be modernised, strengthened and harmonised from source to end markets."

-Third World Wildlife Crime Report, 2024

The advancement of technology and communication in the 21st century is intertwined with ideas of technological rights, such as "digital rights" and "the right to digital security," which come into focus as we navigate this digital age. These rights among the people become more widely recognised in a global society, where having internet access is akin to having a basic human necessity. The foresight of Lawmakers to facilitate legally legitimate online transactions, detect and prevent cybercrimes, and adapt to the ever-evolving digital technologies introduced the Information Technology Act in 2000. This marked a major milestone in integrating technology and legal systems, laying the groundwork for addressing the specific challenges of the digital era. But just as technology advances, so too do the nuances of crimes happen through the internet[3]. Several issues, including data privacy, the replacement of human resources by machines, and the ethical implications of artificial intelligence, raise serious questions about assigning responsibility for the use of technology. These issues are best demonstrated by the dark web, which offers a forum for identity theft, drug trafficking, money laundering, and cyberterrorism.[4]

Cybercrime offences such as Hacking, spam, monetary fraud, money laundering, online blackmailing, child pornography, forgery, drugs, weapons, stolen bank details, hacking activities and identity theft are occurring at an accelerating rate. The darknet and the Dark web are parts of the internet that can be accessed through the TOR browser. Because of providing anonymity, it becomes a platform for illegal activities and makes monitoring complicated for law enforcement.[5] This anonymity has enabled cybercriminals to operate through the dark web, hiding their operations and exposure from the world. However, on the other hand, it serves as a dynamic instrument for governments in sensitive document exchange, or for repressive

3 Dr. Amita Verma, Cyber Crimes in India, 1st ed. 2017, p. 6 (Last visited on 30th December 2024)
4 Raman, Raghu, et al. "Dark web Research: Past, Present, and Future Trends and Mapping to Sustainable Development Goals." Heliyon, vol. 9, no. 11, Nov. 2023, p. e22269. PubMed Central, https://doi.org/10.1016/j.heliyon.2023.e22269.
5 Kumar, A., & Rosenbach, E. (2019). *The Truth About The Dark Web – IMF F&D*. IMF. https://www.imf.org/en/Publications/fandd/issues/2019/09/the-truth-about-the-dark-web-kumar

regimes, while at the same time providing escape routes for dissidents, as many individuals would not want to suffer repercussions if they were to expose themselves.

Criminals increasingly exploit the dark web to evade environmental crimes, particularly through the illegal sale of wildlife and environmental goods. This illicit trade has surged online, particularly during the pandemic, as the internet facilitates anonymous transactions that evade law enforcement. The dark web serves as a marketplace for these activities, where anonymity is enhanced by cryptocurrencies, allowing criminals to obscure their identities while engaging in illegal transactions. The criminals focus on the online illicit trade situation, paralleling its current presence on the surface and deep web, and contemplating its evolution if, by necessity, an increase in law enforcement pushes it into the dark web. Currently, Illicit Wildlife Trade activity on the dark web is minimal. However, along with the increased enforcement, the illicit wildlife trade will also follow a specific pathway, such as moving from the surface/deep web to centralised dark web markets, then to smaller, specialised dark web shops, followed by invitation-only markets, and ultimately, potentially, to distributed peer-to-peer marketplaces. While these shifts will enhance privacy and security for vendors, they will also reduce the overall market size. Through the algorithms and specific customer needs, the effective interventions target the social processes and consumer psychology driving Illicit Wildlife Trade rather than focusing solely on platform control, as such measures merely displace the networks. Back then, Environmental crimes were happening not at a local or zonal level, but globalisation and enhancement have transitioned this issue to the global level.

Thus, it has been estimated that between USD 110 billion and USD 290 billion of illicit profits are generated by criminals, challenging the economic system and impacting the economy. From an ecological perspective, these issues will have a long-term impact on biodiversity and pose a threat to achieving the Sustainable Development Goals. Dullness addressed by the regulatory framework and legislation does not recognise this global issue. Henceforth, legal frameworks at the national and international levels need to be strengthened, utilising coordination amongst law enforcement agencies and to address this issue collectively.[6]

Coupled with Indian laws and international frameworks that have addressed money laundering and environmental offences, India still struggles to effectively regulate, investigate, and

6 Marilyne, Goncalves, and Hart Ailsa. “Handbook on the Compilation of Statistics on Illegal Economic Activities in National Accounts and Balance of Payments.” Following the Money from Environmental Crimes – a Call to Action, 2024, https://blogs.worldbank.org/en/psd/following-the-money-from-environmental-crimes---a-call-to-action.

prosecute crimes facilitated by the dark web's anonymity and decentralised financial systems. The lack of a cohesive legal framework linked with technological and legal challenges hinders the enforcement of anti-money laundering (AML) regulations and environmental protection laws.

Research and Objectives

The perpetrators of crimes often move from the surface web to the deep web. Then to the Dark web due to the anonymity it provides for money laundering and facilitating crimes that are quieter and less likely to be caught by law enforcement. These crimes of environmental significance, whose proceeds go unaccounted for with the use of cryptocurrencies and hidden transactions done through the dark web, imply illegal logging, wildlife trafficking, and unregulated mining. In a context like India, various domestic laws and international instruments have emerged over time to establish legal provisions that focus on mitigating money laundering and environmental offences; however, they face substantial difficulties in regulating, investigating, and prosecuting crimes facilitated by the anonymity provided and the decentralised financial system associated with dark websites. The absence of a coherent legal framework weakens the capability of AML enforcement, along with challenges due to technology and jurisdiction, as well as anti-money laundering regulations and environmental protection laws.

Methodology

This research paper explores the challenges of monitoring environmental crimes and the laundering of illicit products via the dark web. Doctrinal Research methodology is used to analyse and review primary and secondary legal sources, and comparative legal analysis methodology will be employed to examine laws and regulations in India, in order to determine the country's efforts towards this goal. Legal analysis is done in the study to investigate how law enforcement, environmental agencies, and corporations can collaborate to combat money laundering through the dark web, thereby strengthening the legislation and financial transactions.

Comprehensive Situation – Utilisation of the Dark Web as a medium of Illicit activities.

1. **Case of trafficking of endangered species:** In India, there is a significant increase in the trafficking of endangered species like Pangolins and Tigers, which is facilitated through

various social media platforms that extensively include the Dark web. Due to the anonymity afforded to consumers, vendors, and organisers of illegal markets[7]. This anonymity poses difficulties for law enforcement agencies in determining the true identities of wrongdoers. Moreover, due to the availability of illicit wildlife transactions facilitated by certain algorithms and the acknowledgement of law enforcement, crime perpetrators have shifted to the Dark Web, which provides layers of anonymity to web browsers. The government will be aware of these illegal operations going through the dark net but due to a lack of a legal framework that helps to connect the money laundering from Environmental Crimes through the Dark Net, the legal framework should focus and emphasise grabbing the wrongdoers, whether group or at individual level and by doing so would bring the dynamic changes in the legal framework of India.

2. **Case of Wall Street Market and the issue of jurisdiction:** Wall Street Market (WSM), a prominent dark web-based black market that involved illicit goods, including drugs, arms, data, and Illicit wildlife proceeds, with over 1.15 million users and approximately 5,400 vendors, operating through the Tor network. This network provides e-commerce websites utilising encrypted communications, vendors, and virtual currencies. Subsequently, WSM's operations ultimately experienced a downfall due to an attempted $11 million exit scam, which followed its seizure by law enforcement in May 2019 as part of Operation Dark HunTor. These situations led to the arrests of three defendants in Germany, emphasising the importance of international cooperation among agencies like the FBI, DEA, Europol, and law enforcement from multiple countries. The case showcases key legal issues of jurisdiction over foreign nationals violating U.S. laws and the increasing sophistication of evidence gathering against cyber criminals. The downfall of WSM and other such sites disrupted the dark web landscape, emphasising the ongoing efforts to combat transnational cybercrime[8].

7 TRAFFIC. (2019). TRAFFIC Combating Wildlife Crime linked to the internet global trends and China's experiences traffic COMBATING WILDLIFE CRIME LINKED TO THE INTERNET GLOBAL TREND AND CHINA'S EXPERIENCES TRAFFIC. https://www.traffic.org/site/assets/files/12352/combating-wildlife-crime-online-chinas-experiences.pdf

8 Office of Public Affairs, US Department of Justice. (2019, May 3). Three Germans Who Allegedly Operated Dark Web Marketplace with Over 1 Million Users Face U.S. Narcotics and Money Laundering Charges. Justice.gov. https://www.justice.gov/opa/pr/three-germans-who-allegedly-operated-dark-web-marketplace-over-1-million-users-face-us

3. **Case of Tamil Nadu Wildlife Crime Control Bureau and Parthiban, Tamizh**: Through the sources from the Interpol Report, in India, wildlife crime perpetrators via alphanumeric URLs having codes ending with ".onion" and using "ProtonMail" for communication were offering to sell the Tiger Cub on the dark web hidden services[9].

The address to the deficit in the legal framework of India is mentioned in the IT Act 2000, which does not address the inter-jurisdictional complexity of crimes facilitated by the dark web. Also, the Prevention of Money Laundering Act, 2002, expressly does not mentions money laundered through cryptocurrency.

Right To Internet Access: Nexus of Environmental Crimes and Money Laundering Via Dark Web

Due to exposure to social media and the availability of information through the internet, a hybrid marketplace has emerged, offering the alternative distribution of both legal and illegal species and products, including rare and restricted ones. Although the use of the Dark Web in India is legal and legitimate, accessing it is not considered an illegal activity in India. However, accessing illegal activities like Hacking, spam, financial fraud, money laundering, blackmail, child pornography, forgery, drugs, weapons, stolen bank details, hacking activities, and identity theft would end up committing a cognisable offence.[10] Internet access is essential for human development from an economic perspective, due to the increasing recognition of internet access as a fundamental right.[11] Still, it cannot be denied that the dark web provides an opaque and complicated structure for criminals to utilise the platform as a marketplace for illegal Environmental proceeds without direct check from the enforcement.

This platform not only facilitates the laundering of illegal environmental proceeds into the country but also processes financial transactions from these illegal proceeds within the economy. Therefore, a legal and economic aspect must be added to address the economic and environmental risk by utilising open-source intelligence (OSINT), monitoring with algorithms and keywords to track the platform. By combining legal and technological advancements,

9 Wild Hub. (2023, September 10). Unmasking the Dark Web: The Hidden World of Illegal Wildlife Trade. Wild Hub. https://wildhub.community/posts/unmasking-the-darkweb-the-hidden-world-of-illegal-wildlife-trade
10 Rushi, Bhagat. "INTERSECTION OF FOURTH GENERATION RIGHTS AND DIGITAL INSECURITY: DARK WEB THE FACE OF CYBER THREATS ON HUMAN RIGHTS." *GAP iNTERDISCIPLINARITIES*, VII, no. III, 2024, pp. 61–67, https://www.gapinterdisciplinarities.org/articles?issue=37.
11 Faheema Shirin vs State of Kerala, WP(C). No. 19716 of 2019 (L)

criminal activities can be traced by linking the right to internet access, environmental governance, financial transparency, and legal reform.

Challenges and Gaps in Combating Environmental Crimes from the Dark Web

The anonymity used by criminals and the dispersed control over the dark web hinder the implementation of law enforcement, allowing criminals to sell illicit proceeds without revealing their identities and keeping enforcement agencies in turmoil. International and national frameworks are in place to address the issue of the Dark web. Still, they do not address the link between environmental crimes and the Dark web, which is used as a medium to launder illegal proceeds and illicit funds. Although India has been a member of INTERPOL and the United Nations Office on Drugs and Crime since 1949, due to legal inconsistencies and overlapping jurisdictional powers, the effectiveness of resource sharing and the country's collaboration with international institutes has been compromised. The sharing of information can be hindered when two institutions have separate jurisdictional mandates, such as the Central Bureau of Investigation, which can initiate inquiries and investigations based on court orders or directives from the central government. In contrast, the Enforcement Directorate can instigate an inquiry or investigation based on an offence registered under the "schedule" or based on a first information report or based on a lead received from their intel.

Furthermore, law enforcement agencies face the challenge of keeping up with technological advancements, including advanced software and tools, as well as digital forensics, in a way that allows the dark web market to shift from various platforms, from large stages to clusters, without complications and surveillance. Moreover, the challenge to control internet access cannot be achieved through continuous surveillance, which harms public trust and civil liberties.

Suggestions and way ahead to policy Implications

Legal Harmonisation:

The dark web provides anonymity, making it difficult to monitor and prevent the sale of illicit proceeds of Environmental crimes and money laundering and detecting suspicious activities like illegal wildlife trade, illegal trade of logs, use of Pegasus spyware, chrysaor which is similar to Pegasus spyware, Finspy, Hermit, Devils Tongue, Sherlock and cyber scams like Crypto investment fraud, Phishing, "Hello Pervert" scams are facilitated by the Dark web to spy or to keep the surveillance on state and non-state actors, sextortion scams to blackmail

victim for ransom.[12] The government should use real-time data and algorithms to detect the illicit environmental and ecological transactions while protecting the privacy of individuals.[13]

Technological Enhancement:

A study of algorithms based on behaviour and criminology, along with continuous improvement, can help discourage offenders from engaging in such illegal activities. In this domain, it is improbable that such operators will require a high level of stealth, except where the consequences of detection could be terrible. There may be access to some sites only when they come online during specific moments, with brief time frames for trade before they disappear from view, making them challenging for investigators to crack.[14]

Moreover, the Indian government has given the authority via the Indian Cybercrime Coordination Centre (I4C), which acts as the nodal agency to curb, facilitate the lodging of complaints, analyze trends, and create awareness to curb cybercrime in India and help the Enforcement Directorate to attach and confiscate the assets related to crimes.[15]

Conclusion

Tracing money laundering and Environmental crimes through the Dark Web poses a challenge for law enforcement agencies, as the dark web provides privacy and protection from controlling supervision and imposing surveillance; at least these features enable a range of criminal activities such as trafficking illegal goods, money laundering through cryptocurrencies, and the illicit trade in environmental resources. The untraceable nature of digital transactions heightens these challenges, enabling criminals to anonymously convert illicit gains into virtual assets and then launder them through urbane mechanisms such as mixers, internal exchanges, and decentralised platforms. This creates a pressing need for strengthened and harmonised cooperation between law enforcement bodies, financial institutions, and regulators globally to close loopholes and disrupt these illicit financial flows.

12 “Social Media, Dark Web and Cryptocurrencies: Curbing the Illegal Online Sale of Wildlife and Environmental Goods.” Basel Institute on Governance, https://baselgovernance.org/news/social-media-dark-web-and-cryptocurrencies-curbing-illegal-online-sale-wildlife-and.

13 K.S. Puttaswamy vs. Union of India, AIR 2017 SC 4161

14 Rushi, Supra note 9

15 Indian Cybercrime Coordination Centre (I4C). “Indian Cybercrime Coordination Centre (I4C).” Training, Awareness and Capacity Building Programme, Government of India, https://i4c.mha.gov.in/training.aspx.

Additionally, this platform ensures the right to privacy and digital security, as enshrined in the Charter of Human Rights and Principles for the Internet. The regulations and enforcement should be balanced in a way that strikes a balance between criminal activities and the protection of individual interests, including the right to access the internet and the right to privacy. Articles 8 and 9 of the charter not only emphasise the punishment of criminals but also focus on public awareness and education on the complexities of the evolving dark web. Henceforth, it is vital to create public awareness through radio, TV, and advertisement banners by involving microfinance companies, NGO's, influential persons from the panchayat, and self-help groups. Thus, it creates the necessity to make people aware of the advancements in the work of the dark web and the various technologies. Having little or half-knowledge leads to creating more ignorance, whereas not knowing anything can lead the person to caution. Lastly, Humans must adapt over time as technology also continuously advances.