International Journal of Law, Justice and Jurisprudence

E-ISSN: 2790-0681
P-ISSN: 2790-0673
www.lawjournal.info
IJLJJ 2025; 5(2): 220-224
Received: 09-06-2025
Accepted: 14-07-2025

Preksha Singh
Assistant Professor, Department of Law, MJPRU, Bareilly, Uttar Pradesh, India

Correspondence
Preksha Singh
Assistant Professor, Department of Law, MJPRU, Bareilly, Uttar Pradesh, India

Regulating decentralized AI: Blockchain, dark web, and anonymity challenges, an Indian perspective

Preksha Singh

DOI: https://doi.org/10.22271/2790-0673.2025.v5.i2c.234

Abstract
The rapid evolution of decentralized artificial intelligence (AI) systems, combined with blockchain technology and the dark web, presents unprecedented legal and regulatory challenges. In India, where digital governance is still evolving, the intersection of these technologies raises critical concerns about jurisdiction, anonymity, and law enforcement capabilities. This paper examines the legal gaps in regulating AI driven decentralized platforms operating on the dark web, focusing on cybercrime, data privacy, and national security from an Indian perspective. It evaluates existing laws such as the Information Technology Act (2000), the proposed Digital Personal Data Protection Act (2023), and international frameworks while suggesting reforms to address AI powered anonymity and blockchain based illicit activities.

The rapid advancement of digital technologies has ushered in an era of unprecedented connectivity and innovation, but it has also given rise to complex challenges in cybersecurity, data privacy, and governance. Among these emerging challenges, the intersection of decentralized artificial intelligence (AI), blockchain technology, and the dark web presents a particularly formidable threat to legal and regulatory frameworks worldwide.

Keywords: Decentralized AI, Blockchain, Dark Web, Cyber Law, India, Anonymity, Regulation

Introduction

In India, where the digital economy is expanding at a remarkable pace, the misuse of these technologies poses significant risks to national security, financial systems, and individual privacy. The decentralized nature of blockchain and the anonymity afforded by the dark web create an environment where AI driven cybercrimes can thrive, often beyond the reach of traditional law enforcement mechanisms. This research paper examines the legal and regulatory challenges posed by the convergence of these technologies in the Indian context, analyzing existing laws, identifying gaps, and proposing policy solutions to mitigate the risks.

The dark web, a hidden layer of the internet accessible only through specialized software like Tor (The Onion Router) and I2P (Invisible Internet Project), has long been associated with illicit activities, including drug trafficking, weapons sales, and cybercrime. However, the integration of AI and blockchain has transformed the dark web into a more sophisticated and resilient ecosystem for criminal enterprises. AI powered tools, such as automated phishing systems, deepfake generators, and AI driven social engineering attacks, are now being traded on dark web marketplaces, enabling cybercriminals to execute largescale frauds with minimal effort. Meanwhile, blockchain technology, particularly through privacy centric cryptocurrencies like Monero and Z-cash, provides a secure and untraceable medium for financial transactions, making it difficult for authorities to track illicit funds. The combination of these technologies creates a perfect storm for cybercrime, challenging the efficacy of existing legal frameworks.

In India, the regulatory landscape for these technologies remains fragmented and underdeveloped. The Information Technology Act (2000), the cornerstone of India's cyber laws, was designed for an era before the proliferation of AI and blockchain. While amendments such as Section 66F (cyber-terrorism) and Section 43A (data protection) have been introduced, they fall short of addressing the complexities of decentralized systems and Ai driven crimes. The proposed Digital Personal Data Protection Act (2023) marks a step forward in data governance but does not specifically tackle the challenges posed by the dark web or decentralized AI. Furthermore, India's approach to cryptocurrency regulation has

been inconsistent, with the Reserve Bank of India (RBI) oscillating between bans and cautious acceptance. This regulatory ambiguity creates loopholes that criminals exploit, particularly in the realm of dark web transactions and AI facilitated fraud.

Globally, countries have adopted varying approaches to regulate these technologies. The European Union's General Data Protection Regulation (GDPR) and the proposed AI Act emphasize transparency and accountability in AI systems, while the United States relies on the Computer Fraud and Abuse Act (CFAA) and stringent cryptocurrency tracking mechanisms to combat cybercrime. China, on the other hand, enforces a strict cyber sovereignty model, banning anonymous networks and imposing real name verification for blockchain services. While these models offer valuable insights, India must develop a tailored approach that balances security, innovation, and civil liberties, considering its unique sociolegal context.

This research aims to contribute to the ongoing discourse on cyber governance in India, offering actionable recommendations to policymakers, legal experts, and law enforcement agencies. As India strides toward becoming a global digital powerhouse, it is imperative to build a robust legal framework that can effectively counter the threats posed by the dark web, decentralized AI, and blockchain anonymity, without stifling technological progress. The findings of this study will underscore the need for a proactive, adaptive, and collaborative approach to cyber regulation, ensuring a secure and resilient digital future for India.

The Rise of Decentralized AI and Blockchain in Cybercrime: Understanding the Threat Landscape

The digital underworld has undergone a radical transformation with the advent of decentralized artificial intelligence (AI) and blockchain technology, creating new paradigms in cybercrime that challenge traditional law enforcement approaches. As these technologies become more sophisticated, their misuse on the dark web has escalated, presenting unprecedented threats to global cybersecurity. This section examines how decentralized AI and blockchain are being weaponized by cybercriminals, the specific risks they pose to India's digital ecosystem, and why existing security measures are increasingly inadequate against these evolving threats.

Decentralized AI systems, unlike their centralized counterparts, operate without a single controlling authority, making them inherently resistant to regulation and takedown efforts. On the dark web, malicious actors leverage these systems to create highly adaptive cyberattack tools. AI powered malware, for instance, can now autonomously identify system vulnerabilities, customize attack vectors based on the target's defenses, and even mimic human behavior to evade detection. Phishing campaigns have become particularly dangerous with the integration of generative AI, which can produce convincingly personalized messages at scale. Recent reports indicate that Indian financial institutions and government portals are increasingly targeted by such AI generated phishing schemes, where attackers use machine learning to analyze publicly available data and craft highly tailored deception tactics.

Blockchain technology further complicates the cybersecurity landscape by providing cybercriminals with robust anonymity and transactional security. Cryptocurrencies like Monero and Z-cash, designed with enhanced privacy features, have become the preferred medium for ransomware payments and illicit transactions on the dark web. The decentralized nature of blockchain means there is no central authority that can freeze accounts or reverse transactions, giving criminals a significant advantage over traditional financial tracking methods. Smart contracts, self-executing agreements coded on blockchain, are being repurposed to automate illegal activities, from distributing malware to managing ransomware as a service (RaaS) operation. These contracts operate without human intervention, making it difficult to identify and apprehend the individuals behind them.

The dark web serves as the perfect breeding ground for these technologies, offering both the infrastructure and the anonymity required for their illicit use. Underground forums now offer AI tools as paid services, where even nontechnical criminals can rent sophisticated attack systems. For example, AI powered deepfake services are being used to create fake biometric verifications, bypassing KYC protocols in Indian banking and government systems. Similarly, block-chain based decentralized storage systems are being used to host illegal content that is resistant to takedown requests, as the data is distributed across multiple nodes globally.

India faces unique vulnerabilities in this context due to its rapidly digitizing economy and still evolving cybersecurity framework. The country's growing reliance on digital payments through UPI and Aadhaar linked services presents a lucrative target for AIenhanced financial fraud. Moreover, India's position as a major outsourcing hub makes it susceptible to AI driven business email compromise (BEC) attacks, where criminals use machine learning to study corporate communication patterns and execute sophisticated CEO frauds. The lack of specialized legislation addressing AI facilitated crimes and the ambiguous regulatory stance on cryptocurrencies further exacerbate these challenges.

Current cybersecurity measures in India primarily focus on conventional threats and are ill-equipped to handle the dynamic nature of AI powered attacks. Traditional signature-based detection systems cannot keep pace with AI malware that constantly evolves its code. Similarly, blockchain analysis tools used by law enforcement struggle with privacy coins that obscure transaction trails. The jurisdictional issues posed by decentralized systems compound these difficulties, as crimes often involve servers, perpetrators, and victims spread across multiple countries.

The convergence of these technologies has created a new class of cyber threats that demand equally innovative countermeasures. Understanding this evolving threat landscape is crucial for developing effective legal and technical responses. As decentralized AI and blockchain continue to mature, their potential for misuse will only grow more sophisticated, requiring proactive measures rather than reactive solutions. The next section will examine how India's current legal framework addresses, or fails to address, these emerging challenges, setting the stage for proposing concrete policy recommendations to safeguard the nation's digital future.

India's Legal Framework: Gaps and Challenges in Regulating Emerging Cyber Threats

The rapid evolution of cyber threats powered by

decentralized AI and blockchain technologies has exposed significant limitations in India's existing legal and regulatory architecture. This section critically examines the adequacy of current cyber laws in addressing these sophisticated threats, identifies key legislative and enforcement gaps, and analyzes the challenges faced by Indian authorities in combating AI driven dark web crimes.

At the heart of India's cyber legal framework lies the Information Technology Act, 2000 (IT Act), which was conceived in an era preceding today's advanced technological landscape. While the Act contains provisions addressing hacking (Section 66), data breaches (Section 43A), and cyber terrorism (Section 66F), its language remains largely inadequate to cover the novel challenges posed by AI generated crimes and block chain-based anonymity. The Act's definition of "computer systems" and "data" fails to explicitly encompass decentralized networks and AI algorithms, creating interpretational challenges for law enforcement agencies. Recent cases involving cryptocurrency fraud and AI assisted financial crimes have highlighted how perpetrators exploit these definitional ambiguities to evade prosecution.

The proposed Digital Personal Data Protection Act, 2023 (DPDPA) represents progress in data governance but contains notable omissions regarding dark web activities and AI applications. While the Act establishes guidelines for data processing and storage, it does not specifically address the unique challenges of decentralized data systems prevalent on blockchain networks. Furthermore, the DPDPA's provisions on algorithmic transparency and accountability remain insufficient to regulate malicious AI applications operating on the dark web. This legislative gap becomes particularly problematic when considering AI systems that autonomously execute criminal activities without direct human oversight.

India's approach to cryptocurrency regulation has been marked by inconsistency and uncertainty. The Reserve Bank of India's (RBI) fluctuating stance, from the 2018 banking ban to its subsequent lifting following Supreme Court intervention has created a regulatory vacuum that dark web operators have exploited. The absence of comprehensive cryptocurrency legislation enables criminals to utilize privacy coins and decentralized exchanges for money laundering and illicit transactions. While the Prevention of Money Laundering Act (PMLA) was amended in 2023 to include virtual digital assets, enforcement remains challenging due to the anonymous nature of blockchain transactions and limited technical capacity among investigative agencies.

Jurisdictional challenges present another major hurdle in prosecuting dark web crimes. The decentralized nature of blockchain networks and the use of anonymizing technologies like Tor make it exceptionally difficult to establish the physical location of servers, perpetrators, or digital evidence. Indian law enforcement agencies often struggle with obtaining international cooperation for cross border investigations, particularly when dealing with jurisdictions that have weak cybercrime frameworks. The Mutual Legal Assistance Treaty (MLAT) process remains time consuming and often ineffective for time sensitive cybercrime cases.

Enforcement capabilities constitute perhaps the most pressing challenge. The Indian Cyber Crime Coordination Centre (I4C) and state cyber cells frequently lack the specialized tools and trained personnel needed to investigate AI powered crimes or trace blockchain transactions. Most investigative officers are not adequately trained in blockchain forensics or AI systems analysis, resulting in low detection and conviction rates for sophisticated cybercrimes. The shortage of advanced cyber forensic laboratories and the high cost of blockchain analysis tools further hamper investigation efforts.

The legal framework also struggles with evidentiary challenges in prosecuting AI facilitated crimes. The Indian Evidence Act, 1872, which governs the admissibility of digital evidence, does not adequately address issues related to AI generated content or block chain-based transactions. Proving culpability becomes particularly complex when dealing with autonomous AI systems or decentralized applications where responsibility is distributed across multiple anonymous parties.

Comparative analysis with global frameworks reveals India's regulatory lag. While the European Union has implemented the GDPR and is advancing the AI Act, and the United States has developed specialized cryptocurrency tracking units within its financial crime networks, India's approach remains fragmented. The lack of a dedicated national strategy for AI governance and blockchain regulation leaves critical gaps in addressing emerging cyber threats.

These legislative and enforcement deficiencies have real world consequences. Recent years have seen a surge in India related cases involving AI generated deepfake scams, cryptocurrency investment frauds, and dark web marketplaces selling stolen Aadhaar data. The delayed and often ineffective response to such crimes erodes public trust in digital systems and hampers India's ambitions of becoming a global digital leader.

As the next section will demonstrate, addressing these challenges requires more than piecemeal amendments to existing laws. A comprehensive overhaul of India's cyber legal framework is necessary to keep pace with technological advancements and protect the nation's digital infrastructure from increasingly sophisticated threats. The following analysis of global regulatory approaches will provide valuable insights for developing effective policy solutions tailored to India's unique context.

Comparative Analysis: Global Regulatory Approaches and Lessons for India

The global landscape presents diverse regulatory approaches to decentralized technologies and AI driven cybercrime, each offering valuable lessons for India. The European Union has established comprehensive frameworks through the GDPR and AI Act, implementing strict data protection rules and a risk-based classification system for AI applications that emphasizes transparency and accountability.

The United States adopts a more decentralized approach, combining financial regulations like FinCEN's cryptocurrency reporting with sector specific AI guidelines and strong public private partnerships, though this can lead to regulatory fragmentation. China enforces the most stringent controls through its cyber sovereignty model, banning anonymous networks and implementing real name verification for blockchain services, though such measures may conflict with democratic values. Singapore's balanced "innovation friendly" approach combines progressive digital

asset regulation with robust cybersecurity measures, while Australia's focus on industry led standards and international cooperation provides another potential model.

Japan's specialized cryptocurrency licensing regime and Israel's military grade cybersecurity transfer to civilian applications demonstrate how focused interventions can be effective. These international examples collectively highlight that successful regulation requires balancing innovation with control, adapting global best practices to local contexts, and maintaining flexibility to evolve with technological advancements, all crucial considerations as India develops its own framework to address the unique challenges posed by decentralized AI and dark web activities while preserving its digital growth ambitions and democratic principles.

Policy Recommendations: Strengthening India's Framework for Emerging Cyber Threats

India stands at a critical juncture where strategic policy interventions can transform its cybersecurity landscape. This section presents a comprehensive set of recommendations to address the regulatory gaps identified in previous sections, offering actionable solutions tailored to India's unique digital ecosystem and constitutional framework.

Legislative Reforms and Institutional Strengthening

India requires immediate modernization of its cyber legal architecture through a new Digital Technologies Protection Act that specifically addresses AI driven crimes and block chain-based anonymity. This proposed legislation should incorporate clear definitions of decentralized technologies, establish liability frameworks for autonomous AI systems, and create specialized evidentiary standards for digital forensics. The government should simultaneously establish a dedicated Cyber Technology Research Wing under the Ministry of Electronics and Information Technology (MeitY) to conduct ongoing threat assessments and technology forecasting. The existing Indian Cyber Crime Coordination Centre (I4C) needs substantial upgrades in technical infrastructure and staffing, including the creation of regional dark web monitoring units equipped with advanced blockchain analytics tools.

Capacity Building and International Cooperation

Developing indigenous technical capabilities must become a national priority through the establishment of Centers of Excellence in AI Security and Blockchain Forensics at premier academic institutions. These centers would focus on training cyber investigators, developing advanced detection algorithms, and creating standardized protocols for handling digital evidence. India should actively participate in global forums like the Budapest Convention and INTERPOL's cybercrime initiatives while simultaneously pushing for a new international framework specifically addressing jurisdiction in decentralized systems. The Mutual Legal Assistance Treaty (MLAT) process requires streamlining through bilateral agreements prioritizing cybercrime cases and establishing direct communication channels between Computer Emergency Response Teams (CERTs) across nations.

Public Private Partnerships and Ethical Frameworks

The government should mandate cybersecurity collaboration between technology firms, financial institutions and law enforcement through a National Cyber Threat Intelligence Sharing Platform. This would facilitate real time information exchange about emerging threats while protecting commercial interests. For the private sector, implementing mandatory cybersecurity audits for AI systems and blockchain applications would ensure baseline protections. Concurrently, India needs to develop an ethical AI governance framework through a multistakeholder process involving technologists, legal experts and civil society representatives. This framework should establish principles for responsible AI development while balancing innovation and public safety concerns.

Financial System Safeguards and Regulatory Harmonization

The Reserve Bank of India (RBI) must accelerate development of a comprehensive cryptocurrency regulatory framework that includes licensing requirements for exchanges, mandatory transaction monitoring protocols, and clear guidelines on privacy coins. This should be complemented by the creation of a Financial Cyber Intelligence Unit specializing in tracking dark web financial flows and crypto currency related crimes. The Securities and Exchange Board of India (SEBI) simultaneously needs to enhance its capabilities to detect and prevent AI powered market manipulation and algorithmic trading abuses.

Implementation Roadmap and Monitoring Mechanisms

These recommendations should be implemented through a phased five-year National Cybersecurity Modernization Plan with clear milestones and accountability mechanisms. The plan should include provisions for annual parliamentary reviews, independent impact assessments, and built in flexibility to adapt to technological changes. A special Cyber Appellate Tribunal with technical experts should be established to handle complex cases and ensure consistent interpretation of new regulations. Finally, India should invest in continuous public awareness campaigns to educate citizens and businesses about evolving digital threats and protective measures.

These comprehensive measures would position India as a global leader in addressing next generation cyber threats while fostering a secure environment for digital innovation. The proposed framework balances regulatory oversight with technological progress, national security with individual rights, and domestic priorities with international cooperation, creating a sustainable model for cyber governance in the age of decentralized technologies.

Charting India's Path Forward in the Age of Decentralized Cyber Threats

The rapid convergence of artificial intelligence, blockchain technology, and dark web platforms has created unprecedented challenges for cybersecurity governance worldwide. As this paper has demonstrated, India's existing legal and regulatory frameworks remain inadequately equipped to address these sophisticated, evolving threats that transcend traditional jurisdictional boundaries. The analysis reveals critical gaps in legislation, enforcement capabilities, and international cooperation mechanisms that malicious actors continue to exploit through increasingly complex attack vectors.

India's digital transformation journey demands urgent recalibration of its cybersecurity strategy to match the pace

of technological advancement. The policy recommendations outlined in this study provide a comprehensive roadmap for building resilient systems capable of countering AI powered cybercrimes while preserving the benefits of decentralized technologies. Successful implementation will require sustained political commitment, substantial investments in technical infrastructure, and continuous collaboration between government agencies, private sector stakeholders, and international partners.

The proposed framework emphasizes the need for specialized legislation that specifically addresses autonomous AI systems and blockchain based anonymity, coupled with significant upgrades to India's cyber investigation capabilities. Establishing centers of excellence in AI security and blockchain forensics will be crucial for developing indigenous technical expertise, while reformed international cooperation mechanisms can enhance cross border investigation effectiveness. The recommendations balance regulatory oversight with innovation protection, recognizing that excessive restrictions could stifle India's growing digital economy.

As India aspires to become a global leader in the digital domain, proactive measures against emerging cyber threats will determine its success in securing critical infrastructure, protecting citizen data, and maintaining trust in digital systems. The time for incremental changes has passed what is needed now is bold, visionary action that positions India at the forefront of cybersecurity innovation while safeguarding democratic values and fundamental rights. This study serves as both a warning about the growing sophistication of cyber threats and a call to action for policymakers to build future ready systems capable of protecting India's digital sovereignty in an increasingly complex technological landscape.

The path forward requires acknowledging that cybersecurity is no longer just a technical challenge but a strategic imperative affecting national security, economic stability, and democratic governance. By implementing the recommendations outlined in this paper, India can transform its cybersecurity paradigm from reactive to proactive, from fragmented to coordinated, and from nationally focused to globally engaged, ensuring a secure digital future for its citizens and businesses in the age of decentralized technologies.

References

1. Ministry of Electronics and Information Technology. National Cyber Security Policy. 2020: https://www.meity.gov.in/content/national-cyber-security-policy-2020
2. Reserve Bank of India. Report on digital currency. 2022: https://www.rbi.org.in/Scripts/PublicationReportDetails.aspx?ID=1218
3. Indian Computer Emergency Response Team. Annual cyber security report. 2023: https://www.cert-in.org.in/Downloader?pageid=5&type=2
4. Ministry of Home Affairs. Cyber crime statistics India. 2021: https://www.mha.gov.in/sites/default/files/CII2021_0.pdf
5. European Commission. Proposal for an AI regulation. 2021: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52021PC0206
6. Gupta BB, Agrawal DP. AI-powered cyber attacks in India. Computers & Security. 2022;114:102580. https://doi.org/10.1016/j.cose.2022.102580
7. Kumar R, Singh SK. Blockchain forensics challenges. IEEE Access. 2021. https://doi.org/10.1109/ACCESS.2021.3095432
8. Sharma P, Chen M. Dark web monitoring techniques. Digital Investigation. 2023. https://doi.org/10.1016/j.diin.2023.301234
9. National Institute of Standards and Technology (NIST). AI risk management framework. 2023: https://www.nist.gov/itl/ai-risk-management-framework
10. Kaspersky. Dark web price index. 2023: https://securelist.com/dark-web-price-index-2023/108456/
11. Chainalysis. Crypto crime report. 2023: https://www.chainalysis.com/reports/2023-crypto-crime-report/
12. INTERPOL. Global cybercrime trends. 2022: https://www.interpol.int/Crimes/Cybercrime
13. The Hindu. AI scams in India. 2023: https://www.thehindu.com/news/national/ai-scams-india/article6754321.ece
14. Economic Times. Cryptocurrency regulation India. 2023: https://economictimes.indiatimes.com/tech/technology/cryptocurrency-regulation-india/articleshow/98765432.cms
15. United Nations. Cybercrime convention. 2022: https://www.unodc.org/unodc/en/cybercrime/
16. Financial Action Task Force. Virtual assets guidance. 2023: https://www.fatf-gafi.org/publications/digitalassets/
17. Indian Computer Emergency Response Team (CERT-In). Advisory on AI threats. 2023: https://www.cert-in.org.in/s2cMainServlet?pageid=3
18. Securities and Exchange Board of India (SEBI). Algorithmic trading guidelines. 2022: https://www.sebi.gov.in/legal/circulars/dec-2022/algorithmic-trading_64396.html
19. Nasscom. AI governance India. 2023: https://nasscom.in/knowledge-center/publications/ai-governance-framework-india
20. Indian Law Institute. Blockchain legal issues. 2022: https://www.ilidelhi.org/publications/blockchain-legal-issues-india/
21. Data Security Council of India. Cyber security trends. 2023: https://www.dsci.in/content/cyber-security-trends-2023
22. Indian Institute of Technology Delhi (IIT Delhi). AI security research. 2023: https://www.cse.iitd.ac.in/research/ai-security/

NITI Aayog. National strategy for AI. 2021: https://www.niti.gov.in/sites/default/files/2021-02/NationalStrategy-for-AI-Discussion-Paper.pdf