International Journal of Law Research, Education and Social Sciences

Open Access Journal – Copyright © 2026 – ISSN 3048-7501
Editor-in-Chief – Prof. (Dr.) Vageshwari Deswal; Publisher – Sakshi Batham

From Algorithms to Anonymity: The Use of Artificial Intelligence on the Dark Web in India

Shaik Firas Ahmed[a]

[a]NMIMS, Hyderabad, India

Received 17 March 2026; Accepted 17 April 2026; Published 21 April 2026

India's digital ecosystem is experiencing rapid growth in artificial intelligence (AI), and the dark web is also seeing increased use for a range of illicit activities. While the actual dark web is not illegal in itself, its structure, which uses anonymising networks (such as Tor) and is reinforced by cryptocurrencies, provides a platform for many types of illegal activities, including drug trafficking, data breaches, online fraud, botnets, and distributed exploitative materials. When you combine AI with the structures of the dark web, it has made the dark web a significant concern for both local policymakers and law enforcement agencies. At the same time, Indian law enforcement has been using AI-based technologies to detect cybercrime, support digital forensics, enable predictive policing, and identify deep fakes produced with tools such as Generative Adversarial Networks (GANs). Thus, the technology has a dual-use effect, being used by both criminals and state authorities. This has been described by scholars as an 'arms race' relative to the governance of digital data and the management of cybersecurity.

The article illustrates the doctrinal and policy ramifications of the utilisation of artificial intelligence (AI) to facilitate and counter dark web activities in India. This involves examining international and domestic literature on AI-enhanced cyber criminality and identifying current failures in the legal framework for emerging technologies, such as botnets, Generative Adversarial Networks (GANs), and advanced language models. It will pay particular attention to issues of attribution, standards of evidence and cross-border data transfer in the context of changing/novel legal regimes. Judicial developments, including key judicial decisions related to privacy, freedom of speech and digital rights, have influenced where the boundaries of surveillance and enforcement of cyber

activity, by the judiciary/executive, are being established. Continued challenges linking AI-enhanced activity over anonymity to legible persons will be demonstrated by examples of electronic evidence and online crime, where updated evidentiary statutes have placed constraints on the success of such efforts. The purpose of this paper is to advocate for a regulatory framework that is balanced in recognising AI as both a beneficial tool and a harmful tool. India should develop a balanced regulatory framework that is neither overly restrictive nor overly permissive to enhance both the legal and institutional frameworks and promote accountability, transparency, and the protection of fundamental rights. In light of the continuing sophistication of cyber threats, traditional legal mechanisms to address them cannot keep pace with rapidly evolving technology.

Keywords: *artificial intelligence, dark web, information technology, data protection, privacy, electronic evidence.*

INTRODUCTION

In recent times, India has emerged as one of the fastest-growing startup ecosystems worldwide. This growth has significantly contributed to job creation, economic growth, and innovation. Programs such as Startup India, which aim to simplify the process of doing business and promote entrepreneurship, have helped the growth of technology-based businesses. India's rapidly developing digital landscape has revolutionised the way we speak, shop, and govern ourselves. But there are also new forms of technology-based crimes. Recently, the combination of AI and the Dark Web has become an alarming issue for authorities, law enforcers, and scholars. AI technology assists with data processing, automation, and predicting outcomes in the field of law. But when AI technology is misused on the Dark Web, cybercrime becomes more complex. The Dark Web is an encrypted segment of the Internet that requires special tools, such as Tor, to access. It provides users with anonymity, and tracing activities through common detective techniques becomes challenging.

From Algorithms to Anonymity: The Dark Web itself is not illegal, but its design and development are illegal activities, such as the sale of drugs, identity theft, financial fraud, the sale of stolen information, and child sexual abuse images. The addition of AI technology to these Dark Web activities makes it more dangerous. AI-based botnets, GANs, harmful AI models, and phishing activities are examples of AI technology being misused on the Dark Web.

On the other hand, AI technology helps fight crime. The Indian Police Force and other cybercrime authorities are using AI-based tools, including deepfake detection, crime prediction,

and big-data analysis, to track cybercrime patterns. This technology, which criminals misused, has also proved helpful to law enforcement. In this backdrop, it becomes essential to understand the interrelationships among AI technology, Dark Web technology, and India's law-and-order scenario. This article will discuss the use of AI technology on the Dark Web in India and how India's current laws, such as the Information Technology Act 2000 and the Digital Personal Data Protection Act 2023, address the new challenges posed by AI-based cybercrime.[1]

LITERATURE REVIEW

Global scholarship on AI, Botnets and GANS on the Dark web: In the past ten years, there have been a lot of studies done on the dark net and its relationship with cybercrime, illegal trade and private communication using encryption. A review study that mapped out the literature on the dark net and its main topics of discussion showed four main themes were found in studies on the subject:

1. The importance of network security, malware and cyber-attacks;
2. Cybercrime, data privacy and encryption;
3. Machine learning, social media and artificial intelligence;
4. Drug trafficking and cryptocurrencies.

There is some literature discussing the use of Tor, cryptocurrencies, and other tools to facilitate dark web services and untraceable transactions, and how this has made policing more difficult. There has also been literature discussing the use of machine learning to identify dark web illegal trading sites, sort drug sites, and generate intelligence for law enforcement agencies. There has been special emphasis on AI-based malware and botnets. Technical literature has discussed how deep learning and reinforcement learning are used in command-and-control to develop 'self-learning' botnets that evade detection, move laterally, and change tactics in response to detection. There has been literature discussing the use of generative adversarial networks (GANs) to develop 'deepfakes', perfectly realistic images and videos that can be used to commit extortion, spread misinformation, and perpetrate fraud. There has been literature discussing the 'dark side of AI' in cybersecurity: how AI-based algorithms can generate stealthy DNS traffic for

[1] Raghu Raman et al., 'Darkweb research: Past, present, and future trends and mapping to sustainable development goals' (2023) 9(11) Heliyon <https://doi.org/10.1016/j.heliyon.2023.e22269> accessed 15 March 2026

botnets, and how AI-based command-and-control can detect when infected devices come online, thereby increasing network resiliency.[2] There is literature on the dark web and the use of AI to commit cybercrime. There is literature discussing the use of new malicious services that leverage large language models (LLMs) to commit cybercrime. Tools called FraudGPT, WormGPT, and others like them have been offered for subscription on dark web forums and secret channels. They offer chatbots that can create polymorphic malware, BEC scripts, and other social-engineering tools, and can evade content moderation to help less-skilled attackers launch sophisticated campaigns.

INDIA-SPECIFIC WRITING ON THE DARK WEB, THE IT ACT, AND THE DPDP ACT

Indian writings on the dark web primarily discuss existing laws, such as the Information Technology Act 2000 and its 2008 amendments. The writers of these articles observe that there are no special 'dark-web laws' in India, but various sections of the IT Act, as well as other criminal laws, are applied to activities carried out through dark-web networks. The writings observe that using the dark web itself is not illegal. The use of the dark web for illegal activities such as the sale of drugs, weapons, child sexual abuse images, hacking tools, renting botnets, ransomware, the sale of stolen data of India, and the sale of information related to India and Indians is considered illegal under the law.

Writings for the general public state that India has been addressing these illegal activities through Sections of the IT Act (43, 66, 66C, 66D, 66F, 67, 67B) as well as actual crimes under the Bharatiya Nyaya Sanhita and the IPC. The writings observe that India has been addressing these crimes through various agencies, including state cybercrime cells, the CBI, the National Crime Records Bureau (NCRB), the Indian Cybercrime Coordination Centre (I4C), and the Ministry of Home Affairs, with assistance from CERT-In and other cybersecurity firms.

In data protection, experts have characterised the Digital Personal Data Protection Act 2023 as 'the first comprehensive privacy law in India.' 'Digital personal data' is defined, and data protection rules for data custodians are established. These include data protection principles

[2] 'The Dark Web and AI: How Artificial Intelligence is Reshaping Cybercrime and Cybersecurity' (*Webasha,* 01 May 2025) <https://www.webasha.com/blog/the-dark-web-and-ai-how-artificial-intelligence-is-reshaping-cybercrime-and-cybersecurity> accessed 15 March 2026

such as limiting purpose, minimising data, ensuring security, notifying of data breaches, and respecting data subjects' rights. These analyses emphasise that 'DPDP applies to any processing of digital personal data carried out in India or any processing outside India that is for offering goods or services to data principals in India,' which would include many AI services. From the dark web viewpoint, these writings emphasise that 'large data breaches, which often involve the sale of personal data on the dark web, will trigger DPDP regulations, fines, and security practices.'

AI Deepfakes and forensic response in India: Recent research on AI-based threats, such as deepfake scams and the tools to combat them, focused on India. It has been reported that deepfake cybercrime has risen significantly, including scams that trick people into spending money using AI-generated videos of public figures. As a result, the NCRB has partnered with other institutions, such as IIT Delhi and IIT Hyderabad, to develop tools, including 'GAN signature analysis,' that identify hidden marks in AI-generated content to distinguish it from authentic content. [3]This technology has been tested using tools within certain cybercrime organisations. The Law Commission has suggested that digital evidence legislation be adapted to include AI-generated content.

With regard to AI tools, reports indicate that MahaCrimeOS AI, Crime GPT, AI-based CCTV analysis tools, and predictive policing tools are being utilised in various states of India. Although not all of these tools are directed at the dark web, their ability to process and collate evidence makes them pertinent to investigations that intersect the dark web with other crimes.[4]

CONCEPT FRAMEWORK: DARK WEB, AI TOOL AND ANONYMITY

The 'dark web' is an area of the 'deep web' that cannot be indexed by traditional search engines. To access the dark web, users must use specialised software or configure their computer or phone in a particular way. The two most common methods of accessing the dark web are via the Tor network and the Invisible Internet Project. In addition, it is difficult to map a dark web domain

[3] 'What Is GAN Signature Analysis? India's NCRB & IITs Are Using It to Detect Deepfakes Criminals' (*Budding Forensic Expert,* 05 March 2026) <https://www.buddingforensicexpert.in/2026/03/gan-signature-analysis-ncrb-iit-deepfake-detection-india.html> accessed 15 March 2026

[4] Aakriti Bansal, 'Experts at India AI Impact Summit Says No AI Model Can Reliably Detect Deepfakes Yet' (*Medianama,* 18 February 2026) <https://www.medianama.com/2026/02/223-ai-enabled-cybercrime-india-deepfake-threat/ - :~:text="As of now, there is,of synthetic media threats and> accessed 15 March 2026

name to its hosting location. Because of this, as well as the use of cryptocurrency, and privacy enhancing software or services such as VPN's, online activities can be conducted anonymously so many people are drawn to use the dark web anonymously; however, the same anonymity that many users seek out is also desirable to criminals, who use the dark web to buy and sell illegal goods (e.g., drugs, firearms, hacking services, botnet rentals, ransomware, fraud, and child sexual abuse material).

AI tools used in the dark web can be categorised into different types, including:

Botnets & Automated Attack Tools - AI Botnets Utilise Machine Learning for Performing Scan, Select, and Avoid Detection.

Generative Adversarial Network (GAN) - GANs can Produce Synthetic Images, Audio, or Video (Deepfake). As well as to Produce Very Complex Malware to Evade Detection.

Malicious/Criminal Use of (LLM) Language Models and Crime As a Service (CAAS) Types of AI - FraudGPT and WormGPT are two Examples of These Types of Language Models That Are Developed to Create Phishing Emails, Malicious Code, or Social Engineering Scripts, And These Language Models Are Available for Rent on Various Dark-Web Marketplaces.

Defensive AI - Law Enforcement and Cybersecurity Use AI to Identify Unusual Behaviour, Crawl Dark Web, and Use Forensic Toolsets Including GAN Analysis and Image Forensics to Identify Various Situational Awareness Factors.

The anonymity described in this example is not absolute. There is a conditional dependence on the existence of a connection between an activity/sign (such as opinions of a botnet activity pattern or an image generated through GAN technology) and a person's actual existence (e.g., the monetary cost associated with identifying such a connection). This creates an obstacle for defenders attempting to determine these connections using AI to mitigate threats. Conversely, attackers possess an advantage over defenders because they can create AI software that avoids detection while simultaneously mimicking the behaviour of a legitimate user. On the other hand, defenders can develop AI-based programs to detect behavioural anomalies in a manner that identifies attackers through information associated with activities created using GAN technology or DGA technology.

INDIA-SPECIFIC STATUTORY FRAMEWORK, IT ACT, AND DPDP

Offence, Surveillance and Intermediary Liability provisions under the IT Act –

The Information Technology Act 2000, amended in 2008, is the primary legislation for computer crimes, spying powers, and rules for intermediaries in India. The country's crime rules are crucial for managing AI-driven dark web activities.

Section 43 and Section 66 (Unauthorised Access and Computer Crime): Section 43 establishes civil liability for various types of unauthorised access, including stealing information, transmitting viruses, and denial-of-service attacks. Section 66 provides for criminal punishment of the aforementioned acts when they are committed with dishonesty or fraudulent intent. AI botnet networks that transmit distributed denial-of-service (DDoS) attacks against Indian computers, or that steal data from those computers using dark web command-and-control networks, would be subject to this statute.

Section 66C and Section 66D (Identity Theft and Impersonation): Section 66C creates an offence for the fraudulent use of another's electronic signature, password or other identifier. Section 66D creates an offence for committing fraud through the use of computers by impersonating someone else. The use of AI deepfake video or voice cloning technologies to impersonate a government official or family member in an online fraud, regardless of whether the fraud was committed through the dark web, would result in liability under these two statutes and the general fraud laws.

Section 66F (Cyber Terrorism): This statute creates a criminal offence for unauthorised access to information that threatens the sovereignty, security or integrity of India, including the use of AI-enhanced attacks against critical infrastructure through dark web networks.

Section 67 and Section 67B (Obscenity and Child Sexual Abuse Material): These sections state that it is against the law to pass on any obscene/lascivious material, as well as passing on to someone else any obscene/lascivious material using electronic means (including electronic devices). The sections also apply to dark websites that produce and provide AI-powered 'deepfake' pornographic content to Indian victims.

The rules for surveillance and blocking under the law are crucial for managing AI-driven dark web activities:

Section 69 authorises the government to collect, monitor, or access any computer resource for certain reasons. Section 69B authorises the government to monitor or collect traffic data for cybersecurity purposes, and both sections 69 and 69B can be used for lawful traffic analysis or interception of traffic that has been routed through Tor exit nodes, or through VPN gateways or suspected command-and-control servers, provided proper due process has been followed.

Section 69A authorises the government to restrict access to public resources for certain reasons. While section 69A is widely used to block URLs and applications on the surface web, in theory, it could also be used to block gateways or directories that enable access to the dark web.

Section 79 and Intermediaries: Intermediaries are provided with a conditional safety net under Section 79, and the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules of 2021 reinforce this safety net for Intermediaries Hosting or Indexing Dark Web Contents, including links to dark web contents, will lose their safe net if they do not comply with an order from either the government or courts of law. An example of this might be if an Intermediary were to host or index a forum that offers AI-based botnets for rent; they would not have their safe harbour protection if they had hosted or indexed this page.

In the case of Shreya Singhal v Union of India, the Supreme Court has ruled that Section 66A of the IPC makes it an offence to publish 'offensive' messages on the Internet and that Intermediaries do not have to remove any content unless directed to do so by a valid order from the government or courts. When the Supreme Court declares laws that impose restrictions on freedom of speech to be narrowly tailored, Section 69A is a narrow-tailored law, as the blocking of content under Section 69A is not arbitrary, and users or Governmental agencies shall not be able to use Section 69A to block privacy-enhancing technologies such as Tor or other technologies used to engage in criminal acts on the dark web.

Data Protection Duties and State Powers under the DPDP 2023 –

The DPDP Act 2023 establishes a clear process for protecting digital personal data. It establishes obligations for data fiduciaries and confers rights on data principals.

- The DPDP Act 2023[5] applies to digital personal data processed in India and to data processed outside India where it relates to offering goods and services to people in India.
- Data processors must only handle Data Lawfully. They must report to a Data Protection Board (DPB) if they experience a serious security incident. Once you're finished using data for an intended purpose, delete it. You hold no legal obligation to keep hold of personal information.
- You have the right to access records of data processed about you; make changes to them; delete them; withdraw your consent; appoint someone to exercise your data protection rights, if you die or lack the capacity to do so yourself.
- Under DPDP, data processors that do not adhere to the statutory duties set out by the DPDP Act 2023 will incur huge fines for non-compliance, including but not limited to failing to put in place measures to prevent a data breach and/or failing to act on a data breach promptly and accurately.
- The DPDP Act 2023 creates 2 separate points of impact on AI & the Darkweb.
- Data fiduciaries that experience a high rate of data breaches and low levels of data protection (e.g., Data Fiduciaries using AI Data Analytics Tools to protect against Data Breaches) may need to implement new AI-Based Security Analytics Technology to ensure the provision of 'reasonable security'.
- Law enforcement, security agencies and others that use AI-Based Data Analytics Methods to gather data from dark websites in conjunction with an Agency's own data may need to comply with the DPDP Act 2023's State Exemptions provisions or process such data in accordance with Purpose Limitation, Data Minimisation, and Retention Limitation Principles under the DPDP Act 2023.

There are debates about whether bulk data from dark websites can be processed in a manner consistent with DPDP's rights-based model and constitutional privacy requirements.

[5] Digital Personal Data Protection Act 2023

LANDMARK CASES LAW: DIGITAL RIGHTS, CYBER OFFENCES AND ELECTRONIC EVIDENCES

Justice K.S Puttaswamy (Retd) v Union of India (2017):[6] The Supreme Court, with a bench of nine judges, held that the right to privacy is a fundamental right protected under Articles 14, 19, and 21 of the Constitution. The Supreme Court established the proportionality test, under which restrictions on privacy are subject to legislative authorisation, intending to ensure they are legitimate, necessary, and democratic in a country. The judgment recognised informational privacy and encouraged the establishment of a data protection regime to protect citizens from potential harms perpetrated by the government and non-government entities. The judgment in Puttaswamy will serve as a guiding light for AI-driven investigations into the dark web. The measures of mass traffic logging under CERT-In's directions, AI-driven predictive policing, and long-term retention of scraped dark web data will be tested under the Puttaswamy judgment.

Shreya Singhal v Union of India (2015): In Shreya Singhal v Union of India[7], the Supreme Court considered the petitions challenging sections 66A, 69A, and 79 of the IT Act[8]. In this case, it struck down section 66A, which was considered ambiguous and overly broad. Words like 'annoying' or 'grossly offensive' did not meet the standards for restriction set out in Article 19(2). In addition, it also clarified section 79 to the effect that intermediaries can be held liable only if they have been ordered by the court or government to do so. Moreover, it retained the procedure under section 69A, which includes safeguards such as the provision of reasons and a right to review. Shreya Singhal is an important judgment in the context of the dark web, as it restricts the criminalisation of 'offensive' content accessed via tools like the dark web. In addition, it shows that restrictions on technologies like Tor or AI cannot be imposed, as they can be abused.

Anuradha Bhasin v Union of India (2020): In Anuradha Bhasin v Union of India[9], the SC considered whether internet shutdowns and restrictions on movement in Jammu and Kashmir following the scrapping of Article 370 were lawful. The SC found that 'the right to express yourself and the right to work and do business online are constitutional rights,' and shutting

[6] *Justice K S Puttaswamy (Retd) v Union of India* (2019) 1 SCC 1
[7] *Shreya Singhal v Union of India* AIR 2015 SC 1523
[8] Information Technology Act 2000, ss 66A, 69A and 79
[9] *Anuradha Bhasin v Union of India* AIR 2020 SC 1308

down the internet for an indefinite period of time is not permissible under the Constitution. The shutdown must be 'necessary and proportional,' and it must be published and reviewed from time to time.

The government had argued that internet shutdowns were needed because internet usage, including social media and dark web usage, was being used for terrorism and secessionist activities, and that shutdowns were needed to stop this. The SC found that shutdowns should be temporary and reviewed from time to time, and that it was not acceptable to shut down internet access solely because of the risk of dark web use, and that legal measures, possibly with AI to help track and prosecute such use, should be employed instead.

State of Tamil Nadu v Suhas Katti (2004): The case of State of Tamil Nadu v Suhas Katti was one of the first convictions for a cybercrime in India and the first conviction under section 67 of the IT Act for uploading obscene material. In this case, the accused uploaded obscene and defamatory messages about a woman in a Yahoo group. Based on the IP address, email logs, and electronic evidence, the accused was convicted in a brief trial by the Chennai Cyber Crime Cell.

The importance of this case lies in proving that online crimes can be prosecuted under the IT Act and general laws. It also proves how digital evidence can play a crucial role in such prosecutions. Although this case was not related to AI or dark web material, it can still act as a model for future prosecutions involving AI-generated obscene material or CSAM hosted on the dark web.

Anvar P V v P K Basheer (2014) and Arjun Panditrao Khotkar v Kailash Kushanrao Gorantyal (2020): In Anvar P.V. v P.K. Basheer[10], the Supreme Court explained how electronic evidence could be admitted under section 65B of the Indian Evidence Act, 1872 (now replaced by section 63 BSA). The Supreme Court explained that 'if electronic records are produced as secondary evidence, such as copies of CDs, VCDs, etc., they will not be admissible unless they are accompanied by a proper certificate in terms of section 65B(4) issued by a responsible official.' This decision effectively overturned prior decisions that had permitted reliance on oral evidence or documentary evidence in general. The Supreme Court also noted that sections 65A and 65B create a special rule for electronic records, which takes precedence over the general rules.

[10] *Anvar P V v P K Basheer & Ors* AIR 2015 SC 180

In Arjun Panditrao Khotkar v Kailash Kushanrao Gorantyal[11], another three-judge bench reiterated that a certificate in accordance with section 65B(4) is normally required for admission of secondary electronic evidence. However, they also noted that primary electronic evidence is admissible without such a certificate. They explained that this is 'evidence that is contained in or on any device or storage medium that is in the custody or control of a person during the alleged relevant time period; or evidence that is contained in or on any device or storage medium that is found in the alleged relevant time period; or data messages that are stored in a computer server.'

In this latter case, the Supreme Court also noted that difficulties arose in obtaining a certificate from a third party outside the party offering the evidence's control. However, in this regard, there is little room for manoeuvre. After BSA, this is now governed by section 63, which has expanded the certification requirement to more device types and now requires dual certification by a person in charge and an expert. With respect to AI-generated intelligence in dark web cases, such as GAN-generated signature analysis, DGA-generated classifications of botnet traffic, or LLM-generated clustering of marketplace data, this line of authority means that investigators must document how the system works and produce certificates that will hold up in court.

AI TOOLS AND AGAINST THE DARK WEB: BOTNETS, GANS AND LLMS

AI-driven Botnets and Automated Attacks: The use of AI botnets incorporates machine learning into traditional botnet setups to make them last longer and evade detection. Research into botnet detection that focuses on 'Evasion Aware Botnet Detection Using Deep Reinforcement Learning Based GANs for Generation of Synthetic Botnet Traffic' uses deep reinforcement learning-based GANs, like DRLEVGAN, to generate synthetic botnet traffic, making it harder to detect. However, attackers can use this technology to evade detection by designing botnets that bypass both anomaly- and signature-based detection systems, enabling them to conduct DDoS attacks, credential stuffing, and lateral movement in Indian networks with lower detection rates.

According to industry reports, botnets powered by AI are listed as a separate threat alongside dark web and AI threats. This includes the use of self-learning malware that can detect vulnerabilities, adjust its payload, and select the best approach for its attacks. This, combined

[11] *Arjun Panditrao Khotkar v Kailash Kushanrao Gorantyal & Ors* AIR 2020 SC 4908

with the availability of access to compromised Indian corporate networks and credentials for sale on the dark web, makes AI botnets an essential part of the underground economy in India. In fact, reports about the Indian dark web, which focus on threats, also include information about the availability of 'RDP access' and 'corporate shells' for sale.

GANs enabled Deepfakes and Adversarial Malware: GANs are now an essential technology for the development of deep fakes, which are very realistic fake images, audio, and videos, as well as adversarial malware. Studies show that images of malware generated by GANs are effective for testing image-based malware detectors. The GAN images are also distinguishable using well-trained classifiers. The major policy concern regarding GAN technology is that it enables the creation of visual and audio deep fakes that are difficult for humans to distinguish. This leads to fraud, threats, lies, and reputational damage.

In India, there are reports of deepfake scams, and analysis shows that investment scams use deepfake videos of celebrities and other public figures. There are also non-consensual explicit images. The images are available for purchase on the dark web, using GAN models trained on Indian-language and social media images. The NCRB, IIT Delhi, and IIT Hyderabad are working on GAN signature analysis to combat deepfakes by analysing frequency patterns and other minor statistical differences in images generated by GANs. The results show that the images are detected well in laboratory tests.

Malicious LLM and AI Crime-as-a-Service: FraudGPT and WormGPT are concerning technologies based on large language models that appear on dark web forums and Telegram groups, advertising themselves as examples of 'crime as a service' facilitated by AI. Users pay a subscription to access chatbots that can create spear-phishing messages, create templates for business email scams, create invisible malware, or provide advice on breaking into computer systems, all without the safety precautions normally built into most language models.[12]

Even though no specific tool has been named in Indian case law, threat reports from India highlight AI-generated phishing kits, scripts, and templates for social engineering, all targeting Indian banks, fintech, and government portals. The tools are often bundled with consumer data from India, collected from the dark web. The above trends highlight how people in India and

[12] Information Technology Act 2000

beyond could exploit India's digital infrastructure for their own gain. In the realm of defence, Indian law enforcement agencies are experimenting with LLM-based tools such as Crime GPT and MahaCrimeOS AI, which function as investigative copilots, able to access criminal database information, summarise case files, and suggest procedural steps for investigation. The technology behind dark web 'crime bots' is being repurposed within legal bounds to improve police efficiency, raising significant concerns about governance, auditing, and constitutional compliance.

POLICY AND CHALLENGES NORMATIVE CONCERNS IN THE INDIAN CONTEXT

Towards a calibrated Indian Regulatory Framework –

An Indian response to AI on the dark web should be well thought out and focus on the following things: India's effort to address the dark web threat posed by AI technology is a balancing act among many ideas. The IT Act's surveillance powers, CERT-In's broad logging requirements, and the rise of AI technology for facial recognition and predictive policing all make it easy for abuse and mission creep to happen. The dark web's potential for abuse and misuse, along with the dangers posed by AI technology, could lead to violations of privacy and the right to remain anonymous and unknown person for committing illegal activities.

Another contradiction is the skill gaps. Official statistics from the NCRB and the I4C reveal a surge in cybercrime cases, including AI-powered fraud and deepfake scams. This may force the police to rely too heavily on vendor-provided AI technology without a proper understanding of its limitations, accuracy, and potential for bias. On the other hand, the police may be unable to utilise the provisions of the BSA effectively, especially the stringent certification requirements of section 63 of the BSA for complex AI technology outputs.

On the international front, India faces a constraint: the absence of a formal mechanism for international cooperation on dark web investigations, due to its non-membership in the Budapest Convention on Cybercrime, even as it actively engages in other multilateral forums. Threat intelligence suggests the international nature of dark web markets poses a threat to Indian entities. This necessitates robust international cooperation with foreign CERTs, companies, and academic institutions, irrespective of the absence of a treaty.

Explicitly clarifying various provisions of the Indian IT Act apply to AI-generated/mediated actions: Official guidance and if required, amendments to the various statutory provisions in place need to be issued to explicitly state that deploying malicious versions of LLM, AI-generated botnets or GAN-generated deepfakes to commit a crime would be an offence under the following provisions of Sections 66, 66C, 66D, 66F, 67 and 67B of both the IT Act and with it section 3 of the relevant BNS[13] provisions dealing with cheating, organised crime and obscenity.

Incorporating DPDP-compliant Protections into State-level AI utilisation: Law enforcement agencies need to implement rules or standard operating protocols for their AI systems that require compliance with DPDP principles and Putta Swamy's proportionality standard by employing techniques for data minimisation, retention timeframes, population access limitations, and auditing when collecting data from the dark web.

Creating Court Rules for AI Evidence: The High Courts and Supreme Court can use the decisions of Anvar and Arjun Panditrao as a starting point for establishing standards for the admission of evidence generated by Artificial Intelligence (AI). These standards would include the requirement that the methodology used to create the evidence, the error rates associated with that methodology, and the validation studies performed on that methodology be disclosed, either through Practice Directions and/or recommendations from the Law Commission.

Creating an institutional capacity through investments in staff training, establishing specialised cyber forensic labs, acquiring GAN signature analysis equipment, and developing custom AI models for the linguistic and socially technological settings of India are necessary to eliminate the reliance on vendor systems that rely on opaque data and improve the quality of investigations.

Increase Transparency and Accountability: Regularly publicly report AI use in law enforcement, publish CERT-In advisories about AI-enabled threats, and include civil society and academic experts in oversight mechanisms. These steps will reduce fears of surveillance overreach and build public confidence.

[13] Bharatiya Nyaya Sanhita 2023

CONCLUSION

The incorporation of AI and the convergence of the dark web have altered India's cybercrime landscape, increasing the sophistication of attacks and the complexity of legal responses. AI-based botnets, GAN-based deepfakes, and malicious LLMs on the dark web lower the barriers to committing high-impact cyber offences against Indian individuals and organisations, while also providing defenders with new analytical and forensic capabilities to counter these threats. The core IT Act and DPDP Acts, together with the BSA and CERT-In Directions will provide a legal framework for responding to these kinds of cyber offences in India; however, their effective implementation will require a careful interpretation of statutes, building the capacity of law enforcement and regulatory authorities, and aligning with constitutional jurisprudence on privacy, free speech and due process as expressed in Puttaswamy, Shreya Singhal and Anuradh Bhasin.[Hence, forward-looking regulations should take an approach to regulating AI that views it as both an investigative tool that can aid criminal matters and a tool that may become nothing but a threat to the public. Thus, AI is a dual-use technology that will require an appropriate regulatory structure to govern its use in the investigation and prosecution of crime.

If the IT Act's definitions of AI-mediated dark-web conduct are clarified and all future uses of AI by government agencies include operational safeguards compliant with DPDP, evidential standards are established for AI-generated evidence, and sufficient capacities for the transparent and accountable use of AI by law enforcement agencies in India are developed; then the potential for AI to assist in the identification of otherwise anonymous individuals or entities will exist. At the same time, the Constitution's commitments to dignity, autonomy and the rule of law will continue to exist in an online society that evolves digitally.