Page: 47-68 *URL: www.lijdlr.com*

LAWFOYER INTERNATIONAL JOURNAL OF DOCTRINAL LEGAL RESEARCH

ISSN: 2583-7753

LawFoyer International Journal of Doctrinal Legal Research

[ISSN: 2583-7753]

Volume 3 | Issue 2

2025

DOI: https://doi.org/10.70183/lijdlr.2025.v03.41

AI: A NEW TERROR UNLEASHED

Bhoomi Jain[1]

I. ABSTRACT

Artificial Intelligence is the study and development of computer systems that can copy intelligent human behavior.[2] *With the new intelligent machines that enables a high level cognitive process accompanied with the data subscription, AI has presented an opportunity to supplement the human lives and make it easy for them to live their lives more luxuriously. But the increased use of AI has been supplemented by the potential risks associated with it, such as deep fake videos, dark web, online bots to negatively influence the opinion of the public etc. The rapid growth of AI is not only transforming various sectors but is also bringing new legal challenges, especially in the globe of cyber laws and traditional notions of mens rea and vicarious liability. Thus, this paper critically investigates paradoxical impact of AI on Indian cyber jurisprudence. The study analyses various legal frameworks along with judicial precedents and a comparative analyses of recent case studies. The paper begins by inspecting the inadequacy of the present statutory frameworks to subject liability in AI driven offences. The paper also gives a comparative analyses of EU, USA and China and India's AI governance. Later, it also enlists some guidelines as to how can the nation adopt strict liability structure for AI operators and also enumerates certain advantages of AI if used in justice delivery system.*

II. KEYWORDS

Artificial Intelligence, Dark Web, Criminal Prosecution, Liability, Indian Cyber Law, Legal Framework

III. INTRODUCTION

AI is a catchall term for a set of technologies that make computers do things that are ought to require intelligence when done by people.[3] In simple terms, AI refers to the consortium of technologies that facilitates the machines to act with a higher level of

[1] Student at Vivekananda Institute of Professional Studies, affiliated with Guru Gobind Singh Indraprastha University

[2] *Oxford Advanced Learner's Dictionary* (11th ed. 2010), https://www.oxfordlearnersdictionaries.com/ (last visited January 10, 2025).

[3] *MIT Technology Review*, https://www.technologyreview.com/ (last visited January 12, 2025).

intelligence coupled with the human version of comprehending, understanding and analyzing a situation. The world has seen AI spreading to every sector of the world. E.g.- from automated flight bookings to language translations often strengthening its influence[4]. These notable developments are more based on machine learning algorithms that are trained with extensive datasets that enable it to produce predictive performances.[5]

The world can easily conclude that AI is not a technology of future rather it has already taken birth contributing to evolution in healthcare, education etc.[6] Computers and the artificial intelligence has changed our view to see the world despite the fact that this technology has very recent history and also it is mandatory to notice that there are no signs as to these technologies hitting their end soon. Ranging from the personal assistance like Siri or Alexa to the newly invented self-driving cars, AI is successful in transforming the daily lives of people and providing new opportunities to develop their standard of living. Nonetheless, what one fails to notice is the negative impact of this technology in the lives of the people.

Many people have noticed that whenever one searches anything from the web or likes a particular video on any social media, the feed of that person starts showing the similar results on all the social media platforms. This is what is known as the infringement of privacy of the person.[7] The benefits, potentials and the uses of the AI cannot be doubted but what cannot be also overlooked is the potential harmful effects of the same in the global era.

Artificial Intelligence is capable of introducing new risks and legal complexities[8]. The vast amount of data that is collected by the AI can lead to the privacy violations if not supervised properly. These data can include personal information that also raises concerns about the consent and privacy infringement of a person and its potential of

[4] Stuart Russell & Peter Norvig, *Artificial Intelligence: A Modern Approach* 2–3 (4th ed. 2020)
[5] Ian Goodfellow, Yoshua Bengio & Aaron Courville, *Deep Learning* 1–20 (2016).
[6] Erik Brynjolfsson & Andrew McAfee, *The Second Machine Age: Work, Progress, and Prosperity in a Time of Brilliant Technologies* 39–45 (2014)
[7] Shoshana Zuboff, *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power* 209–224 (2019).
[8] C. Cath et al., *Artificial Intelligence and the 'Good Society': The US, EU, and UK Approach*, 24 Sci. & Eng'g Ethics 505, 505–28 (2018).

misuse.[9] The AI sponsored surveillance systems are also capable to infringe the individual's privacy rights, navigating to the social, legal and the ethnic plight.

This new development has caused the regulatory gaps through the absence of the provisions specifically relating to Artificial Intelligence. It can be easily observed that the current legislations were not designed with taking AI into consideration that leads to the difficulties in applying the traditional laws to the current AI related crimes.[10] This can straight away result in the erratic enforcement obstacle.

As the technology of AI is raising, it is helping the nation to give rise to new dynasty of criminals who had wrongfully used the AI algorithms to give a rise to new cybercrimes, hackings and various forbidden activities. The major advantage of the AI system is failure to be detected.[11] The criminals tends to anonymize the technologies and the AI evasion techniques which makes it a challenge for the armed forces to trail the origins of the assail.

The utilization of AI generated sham content, such as deepfakes, elevates additional challenges for India's juridical order. Deepfakes have the possibility to falsify evidence, smear reputations, and circulate misleading information, substantially colliding into the integrity of legal framework.[12] Discovering the accuracy of proofs and ensuring the precision of information become foremost trouble for courts and solicitors. Legal professionals need to be cautious in acknowledging and challenging the honesty of AI composed content to safeguard the virtue of the legal processes.[13] Lawbreakers can manipulate AI algorithms to distinguish frailties and susceptibility in economic systems, assisting money laundering, deception, and other cash washing schemes.[14]

[9] Mariarosaria Taddeo & Luciano Floridi, *How AI Can Be a Force for Good*, 361 Science 751, 751–52 (2018).
[10] Ugo Pagallo, *The Laws of Robots: Crimes, Contracts, and Torts* 58–62 (2013).
[11] T.C. King, N. Aggarwal, M. Taddeo & L. Floridi, *Artificial Intelligence Crime: An Interdisciplinary Analysis of Foreseeable Threats and Solutions*, 28 Sci. & Eng'g Ethics 1, 1–25 (2022)
[12] T.C. Helmus, *Artificial Intelligence, Deepfakes, and Disinformation: A Primer* (RAND Corp. 2022)
[13] Thomas C. King et al., *Artificial Intelligence Crime: An Interdisciplinary Analysis of Foreseeable Threats and Solutions*, 27 Sci. & Eng'g Ethics 10 (2021)
[14] S. Seth, *Machine Learning and Artificial Intelligence: Interactions with the Right to Privacy*, 52 Econ. & Pol. Wkly. 66 (2017).

Discovering and accusing such crimes may oblige technical legal expertise and insights of the knotty AI driven aptitudes employed by hoodlums. Bolstering India's fiscal regulations and cooperation with international equivalents to battle against over border economic crimes are fundamental steps in softening this menace. The legal fraternity must also contemplate the comprehensive ethical consequences of AI's engagement in unauthorized activities. The conscientiously just development of AI algorithms is pivotal in securing that these technologies are untapped to perpetrate crimes or damage folks and league at large.

As the AI technics advances, so does the conception of autonomous weapons.[15] Though still not prevalent in India, the potential exploitation of AI in the advancement of autonomous weapons hoists grave statutory and ethical concerns. Such arsenals could function by excluding any human mediation, leading to fortuitous repercussions and random attacks. The legal fraternity must be cautious while monitoring the international progress in relation with AI driven weapons and must fight for robust regulations to hinder their abuse.

Dealing with AI's engagement in criminal areas need a cooperative effort from legal eagles, AI inventors and local society. India's legal world should be alert at the forefront of breakthrough technologies and be quick in adjusting to the developing terrain of AI driven offences. Regular policy analysis and adaptation are compulsory to keep up with the swiftly changing technological geography and to secure that India's legal structure remains powerful in overcoming AI related criminal activities.[16] To boost novelty and progress while safeguarding against AI's abuse, India needs to knock a fragile balance between fostering technological growth and maintaining stringent legal controls. This balance will assist the juridical system to address potentially to developing AI driven intimidation without suffocating technological advancement or violating on individual rights.[17]

Furthermore, nurturing international partnership and data sharing will be essential to review the transnational character of cybercrime and AI-related heinous activities.

[15] N. Leys, *Autonomous Weapon Systems and International Crises*, 12 Strategic Stud. Q. 48 (2018).
[16] Ugo Pagallo, *The Laws of Robots: Crimes, Contracts, and Torts* 117 (2013)
[17] L.M. Martín et al. (eds.), *Artificial Intelligence and Human Rights* (1st ed. 2021).

AI's involvement in criminal affairs in India presents countless legal obstructions that calls a proactive and holistic approach from the legal team. As AI technology endures to advance, it is vital to continuously evaluate and modify legal perspectives to overcome the ever changing terrain of AI driven crimes. Ensuring a balance between innovation and direction is essential in harnessing the advantages of AI while mitigating its mishaps for illegal purposes. By addressing these hindrances head-on and working collaboratively, India can establish a vigorous legal framework that protects from AI related criminal offences while fostering technological progress for the larger good of society.

IV. CHALLENGES IN CRIMINAL PROSECUTION IN INDIA

In India, the criminal liability is the cornerstone of its legal system, defining the scenarios where the individuals can be held accountable for the illegal activities which violate the law. The criminal liability in India for committing these offences are mostly punished by imposing life imprisonment, fines, death penalties or other punishment deemed fit as per law. There are the basic principles for determining the liability for these offences through various statutes, case laws, precedents, constitutional provisions[18]. The essential element of a crime is Mens rea which refers to the "guilty mind"[19]. It entails that the individual acted with malicious intention or a guilty mind, either intending to commit the offense or have reason to believe that the nature of his action is unlawful. Mens rea helps questioning the intention behind the act, prompting the stringency of the punishment.

However, the primary challenge that is faced by the legal system in attributing the criminal liability, is the sufficiency of AI algorithms which are operated independently without any human intervention, cluttering the traditional line of legal prosecution of a person on the basis of the human intention.[20]

[18] C. Eggett, *The Role of Principles and General Principles in the 'Constitutional Processes' of International Law*, 66 Neth. Int'l L. Rev. 197 (2019).
[19] *Legal Dictionary*, *Mens Rea Meaning in Law* (2023), https://www.law.cornell.edu/wex/mens_rea (last visited May 10, 2025).
[20] E. Gruodytė & P. Čerka, *Artificial Intelligence as a Subject of Criminal Law: A Corporate Liability Model Perspective*, in *Smart Technologies and Fundamental Rights* ch. 11 (2020).

In India, the criminal liability is not only extended to individuals but rather also includes some entities such as the corporations. This system refers to the vicarious liability where the company is bound to be legally accountable for any wrong committed its employee in the discharge of its official duty.

However, the recent development of the various technologies has posed the second major challenge faced by the juridical system i.e. the absence of legal personhood imposed on the AI. This failure further complicates the matter, as in India, unlike the living person, there is no criminal liability imposed on the AI. As a result of which AI is not suitable enough to be attributed a status of an independent entity with rights and liabilities conferred on it.[21]

Therefore, the major question that arises out of the offences involving AI is that who should be burdened with the criminal liability and should be awarded the punishment. Nonetheless, there are certain blueprints to surrogate the Information Technology Act with the Digital India Act[22] to encompass the present challenge.[23]

The Indian Penal Code (IPC), 1860 is the statute that decides the criminal liabilities on individuals in India. This act not only defines the nature of a crime, but, on the other hand, it also provides some exception that can be used as defence against criminal liability such as self-defence, insanity, involuntary intoxication and mistake of fact[24]. The structure identifies a prime principle i.e. presumption of innocence until proven guilty, with the onus of burden of proof on the prosecution and ensures fair trial rights of the accused which includes the Right to remain silent, legal representation and Right to speedy public trial.

The subject generated by AI can further intensify the criminal trials by exploiting and manipulating the evidence and elevating suspicions about its genuineness. The

[21] S. Chopra & L.F. White, *A Legal Theory for Autonomous Artificial Agents* (2011).
[22] Ministry of Electronics & Information Technology, *Draft Digital India Act Discussion Paper* (2023), https://www.meity.gov.in (last visited May 10, 2025).
[23] S. Chauriha, *How the Digital India Act Will Shape the Future of the Country's Cyber Landscape*, *The Hindu* (2023), https://www.thehindu.com (last visited May 10, 2025).
[24] A. Kilara, *Justification and Excuse in the Criminal Law: Defences under the Indian Penal Code*, 19 Student B. Rev. 12 (2007).

legalisation must assimilate measures to oppose such deception and secure the morality of evidence in the digital era.

With the increasing use of AI, there are also several raised concerns about the unauthorized access and misuse of personal data. To face these challenges Indian legal system is in dire need to enact certain data protection laws.

The opaque decision making structure of anonymous AI algorithms, specifically those based on deep knowledge and networks, makes it rigorous to understand how these systems debark at concrete decisions and actions.[25] The ambiguity complicates efforts to adjudicate the cause and accountability in AI driven criminal offences, making it formidable to ascribe criminal liability.

For example, in situations where AI systems are integrated into autonomous vehicles or smart traffic mechanisms, and an accident results in loss of life, the legal dilemma arises over whether criminal liability should rest with the AI developer, the vehicle owner, or the system integrator. This legal ambiguity was foreshadowed in Shriram Food and Fertilizer Industries v. Union of India[26], where the Supreme Court applied the doctrine of strict liability in cases involving hazardous technology and public safety. Although not AI-specific, the case provides a jurisprudential foundation for assigning responsibility where advanced technology causes harm without direct human intervention.

Moreover, ensuring the authenticity of digital evidence in such cases is critical. The challenges of admissibility, integrity, and manipulation of electronic records were dealt with in Anvar P.V. v. P.K. Basheer[27], where the Supreme Court laid down the mandatory requirement of compliance with Section 65B of the Indian Evidence Act for electronic evidence. These precedents, though arising in different technological contexts, underscore the need for tailored evidentiary and liability rules as India increasingly confronts AI-related harms.

[25] R.F. Richbourg, Deep Learning*: Measure Twice, Cut Once* (Institute for Defense Analyses 2018).
[26] *M.C. Mehta v. Union of India*, (1987) 1 SCC 395.
[27] Anwar P.V. v P.K. Basheer, (2014) 10 SCC 473.

Data confidentiality and safety grounds also hinder with criminal charges when it arrives to AI. Offenders can use AI algorithms to shortlist and misuse personal data, leading to disastrous consequences for organizations. Fortifying laws of privacy and assuring robust cyber safety measures are vital to guard individuals' privacy rights and preclude AI's participation in criminal activities linked to data handling and exploitation. Confronting the obstructions of associating criminal liability to AI in India mandates a multi-faceted approach. The question in ascribing criminal liability to AI in India are complex and multifaceted.

V. INSIGHTS FROM THE EU, US, AND CHINA TO INFORM INDIA'S AI GOVERNANCE

A comparative analysis of AI regulation across global jurisdictions is essential to contextualize India's emerging legal framework[28]. Countries like the European Union, the United States, and China have taken distinct yet instructive approaches for regulating AI. The EU's Artificial Intelligence Act[29] emphasizes a risk-based approach, classifying AI systems based on their potential harm and enforcing strict compliance, especially in high-risk sectors like healthcare and law enforcement.

The United States[30], while lacking a comprehensive federal AI law, focuses on sector-specific guidelines and voluntary frameworks, encouraging innovation with minimal regulation. China[31], on the other hand, has prioritized state control and ethical governance, mandating algorithmic transparency and responsibility through

[28] Y. Bajpai, *Regulation of Risks Associated with Usage of Artificial Intelligence: A Comparison of the Regulatory Regime Between India and the European Union*, 6 Int'l J. Legal Sci. & Innovation 13, 13–25 (2024), https://ijlsi.com/paper/regulation-of-risks-associated-with-usage-of-artificial-intelligence-a-comparison-of-the-regulatory-regime-between-india-and-the-european-union/ (last visited May 10, 2025).

[29] European Commission, *Proposal for a Regulation Laying Down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act)*, COM (2021) 206 final (Apr. 21, 2021), , https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52021PC0206 (last visited May 10, 2025).

[30] U.S. Gov't Accountability Off., *Artificial Intelligence: Emerging Opportunities, Challenges, and Implications for Policy and Research* (2021), https://www.gao.gov/products/gao-21-519sp (last visited May 10, 2025).

[31] N. Kobie, *China's AI Regulation: What the Rest of the World Can Learn*, *Wired UK* (2022), https://www.wired.co.uk/article/china-ai-regulation (last visited May 10, 2025)

centralized oversight. Each of these models reflects unique political, economic, and cultural values, offering valuable lessons for India.

For India, studying these international models provides an opportunity to craft a balanced and context-sensitive AI regulatory strategy. A hybrid approach could incorporate the EU's focus on human rights and accountability, the US's innovation-driven flexibility, and China's emphasis on algorithmic monitoring. Given India's diverse population, democratic values, and increasing reliance on AI in public services, its regulatory framework must promote ethical innovation while safeguarding privacy, fairness, and transparency. Drawing on global best practices can help India avoid the pitfalls of under-regulation or overreach, and position itself as a leader in responsible AI governance in the Global South.

VI. PROPOSED GUIDELINES FOR ENFORCING PENAL LIABILITIES ON AI IN INDIA

The proposed regulatory guidelines are addressed in order to persue the exclusive disputes constituted by the incorporation of AI mechanics into leading sectors, comprising illegal operations. As AI persists to boost and turn more sovereign, it becomes indispensable to develop a transparent regulatory framework that holds liable the pertinent human actors engaged in the expansion, placement, and usage of AI technics.

Firstly, One suggested criterion is to highlight the doctrine of strict liability, wherein the AI promoters and managers can be retained criminally accountable for AI-driven deeds, regardless of intention or knowledge of the offensive conduct. This procedure emphasises the obligation of humans in securing that AI algorithms are designed and employed maturely to impede any deliberate abuse for criminal purposes. By imposing strict liability on contractors and operators, this measure targets to foster dependable AI evolution exercises, raising openness and obligation in the AI business in India.[32]

[32] H. Sayyed, *Artificial Intelligence and Criminal Liability in India: Exploring Legal Implications and Challenges*, 10 Cogent Soc. Sci. 2343195 (2024), https://doi.org/10.1080/23311886.2024.2343195.

A foundational basis for this in Indian law can be found in the Oleum Gas Leak Case (*M.C. Mehta v. Union of India*)[33], where the Supreme Court established the principle of strict liability for enterprises engaged in hazardous or inherently dangerous activities. The Court held that such entities must ensure no harm is caused, and they cannot plead lack of negligence or foreseeability as a defense. Similarly, in the context of AI, where algorithms can act autonomously with unpredictable consequences, strict liability would compel developers and operators to adopt higher safety and ethical standards.

This proposed adaptation aims to foster responsible innovation by emphasizing accountability, transparency, and due diligence in AI system deployment. It aligns with the evolving need to update tort principles and criminal liability frameworks in response to emerging technologies. By embedding this doctrine within India's AI regulation, legal clarity and public safety could be significantly strengthened

Secondly, proposed guideline for AI lawbreaker liability in India may emphasise on setting clear policies for interpretability and transparency in AI systems. By compelling the developers and operators to facilitate thorough certification and traceability records of AI methods, the juridical system can better comprehend the decision-making courses of AI, specifically in situations concerning criminal activities. This criterion safeguards that the instruments and justification behind AI-driven actions are transparent, allowing juridical professionals to evaluate the magnitude of human participation and obligation in AI-driven violations. Transparency scales provides for constructing public believe in AI techs while guaranteeing equity and liability in ascribing criminal liability.[34]

Thirdly, The AI technic should be granted the legal personhood so that it can bear the direct liability as that of a corporation. Since, some AI mechanics are capable enough to be processed automatically without any use of human, therefore granting the legal

[33] M.C. Mehta v Union of India (1987) 1 SCC 395.
[34] H. Sayyed, *Artificial Intelligence and Criminal Liability in India: Exploring Legal Implications and Challenges*, 10 Cogent Soc. Sci. 2343195 (2024), https://doi.org/10.1080/23311886.2024.2343195.

personhood to AI would help the nation to recognise the illegal liability of certain AI systems.[35]

However, attributing constitutional rights and duties to AI could conflict with fundamental rights—such as the right to equality (Article 14) and freedom of expression (Article 19)—which are inherently anthropocentric. Questions would arise as to whether AI systems could be punished, rehabilitated, or held morally culpable—central pillars of Indian criminal jurisprudence based on mens rea**.**

Furthermore, there should be enforcement of extensive data protection laws as it is vital in proposing administrative measures for AI felonius liability in India. These statutes aims to protect individuals' personal data from any illegal misuse or unsanctioned access by AI systems. By cherishing data privacy and security laws, India can alleviate the hazard of AI being abused by criminals to crop and mishandle sensitive data for offensive purposes. Fortifying cyber security procedures also performs a crucial role in avoiding data infractions that could jeopardize the secrecy and security of individuals and organizations, thereby diminishing the potential for AI engagement in criminal activities in relation with the data control and exploitation.

Supreme Court in a famous 2017 landmark judgement, Justice K.S. Puttuswamy vs Union of India[36], which affirms privacy as a fundamental right under Article 21, directly links to AI regulation by emphasizing the need to safeguard individuals' personal data in the digital age.

The judgment's focus on *informed consent* is particularly relevant, as AI systems often collect and process vast amounts of personal information. It underscores the necessity for AI systems to ensure transparency, giving users clear control over their data. Moreover, the ruling stresses the ethical responsibility of state and private entities in upholding privacy, which aligns with the need for ethical AI development—ensuring that AI does not violate privacy, remains unbiased, and respects individual rights. The judgment also calls for awareness of privacy rights, which can be applied to AI regulation by promoting public education and incorporating privacy principles into

[35] C. Amidei, D.G. Mazzotta & J. Piñera, *Personhood and Artificial Intelligence* (Palgrave Macmillan 2021).
[36] *K.S. Puttaswamy v. Union of India*, (2017) 10 SCC 1

school and college curriculam[37], ensuring that individuals are equipped to protect their privacy in an increasingly AI-driven world

In order to resolve the moral opinions in AI criminal liability, proposed key policy measures may incorporate notifications for liable AI development practices. This measure pressurizes that AI techs should be advanced and deployed in a way that endorses virtuous principles and collective beliefs, minimising the likelihood of AI-driven criminal acts. By supporting ethical frameworks for AI, the legal arena can guarantee that AI technologies are manufactured to minimize prejudices and push fair and neutralising outcomes, especially in criminal justice applications.

VII. HARNESSING THE POWER OF AI: ADVANCING JUSTICE THROUGH INTELLIGENT ENFORCEMENT AND LEGAL INNOVATION

While much of the discourse around Artificial Intelligence (AI) in law enforcement emphasizes its risks, it is equally important to acknowledge its transformative potential.

A. Enhancing Investigative Efficiency in Law Enforcement

AI technologies are revolutionizing law enforcement by improving investigative processes. For instance, AI can analyze vast amounts of data swiftly, aiding in identifying patterns and predicting criminal activities. The National Institute of Justice highlights how AI assists in forensic DNA testing and surveillance, enhancing the accuracy and speed of criminal investigations.[38]

B. Streamlining Legal Processes and Improving Access to Justice

In the legal domain, AI is streamlining processes by automating routine tasks such as document review and legal research. This not only reduces the workload on legal professionals but also lowers costs, making legal services more accessible. Research

[37] Ministry of Educ., *National Education Policy 2020* (Gov't of India 2020), https://www.education.gov.in/sites/upload_files/mhrd/files/NEP_Final_English_0.pdf (last visited May 10, 2025).

[38] Nat'l Inst. of Just., *Using Artificial Intelligence to Address Criminal Justice Needs* (2018), https://www.ojp.gov/pdffiles1/nij/252038.pdf (last visited May 10, 2025)

indicates that AI can enhance the efficiency of legal systems, contributing to more equitable and timely justice delivery.[39]

C. Promoting Transparency and Fairness in Legal Proceedings

AI has the potential to promote transparency and fairness within legal systems. By analyzing large datasets, AI can help identify biases and inconsistencies in legal decisions, supporting efforts to uphold justice and equality. The United Nations University discusses how AI can enhance the fairness and accessibility of legal systems while acknowledging the ethical considerations involved.[40]

VIII. THE ROLE OF AI IN DARKWEB

The dark web, which refers to encrypted online content that is not indexed by conventional search engines and requires specific software, configurations, or authorization to access[41], surrounds segments of the internet that can only be approached using specified web browsers because the details stored on the dark web is not easily approachable, the dark web has an inferior architecture with suburbanised implementation and is often utilised for unlawful activities. The dark web is a significant hazard to organizations that elect to overlook it because both expert and novice threat actors can sail this surreptitious medium and procure information that they can then abuse.

Some of the examples of AI tools or systems[42] currently being used in dark web monitoring are:

- **Memex**, developed by DARPA, which uses AI to analyze relationships across websites and uncover illegal activities hidden in the dark web.

[39] I. Atrey , *The Intersection of Artificial Intelligence and Law* (2023), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4632440 (last visited May 10, 2025)
[40] T. Marwala, *AI and the Law – Navigating the Future Together* (2024), United Nations Univ., https://unu.edu/article/ai-and-law-navigating-future-together (last visited May 10, 2025).
[41] Oxford Univ. Press, *Dark Web*, *Oxford Reference*, https://www.oxfordreference.com/ (last visited May 10, 2025).
[42] Mayank Kejriwal, Jiayuan Ding, Runqi Shao, Anoop Kumar & Pedro Szekely, *FlagIt: A System for Minimally Supervised Human Trafficking Indicator Mining* (2017), arXiv Preprint arXiv:1712.03086, https://arxiv.org/abs/1712.03086 (last visited May 10, 2025)

- **IBM i2 Analyst's Notebook**, which integrates AI-driven analytics for crime pattern detection, often used by law enforcement.
- **Darknet AI**, a project integrating machine learning to detect human trafficking patterns on Tor-based marketplaces.

So the question that floats is the meaning of "dark web monitoring". Basically, it is the system that utilizes both AI and human intelligence, baseline data from across the dark web is collected and then analyzed. Any evidence that is oozed, perceptive, or robbed from one's organization is studied and reported to the cybersecurity team, that permits for immediate directions to mitigate the prevalent threat. The role of AI in the dark web is multifarious and diverse, colliding with certain aspects where it can exacerbate certain negative impacts in the world of dark web.

- **Augmented Criminal Activities**[43]**:** AI tools can be utilized to computerise and maximise unlawful activities, such as the development of phishing scams, the advancement of malware, and the facilitation of illicit drug trafficking. To cite, machine learning algorithms can investigate enormous amounts of facts to distinguish susceptibility in systems or fortell consumer trends for illicit goods.
- **Anonymity Corrosion**[44]**:** AI can conceivably weaken the obscurity that the dark web tenders by enhancing the competence of law execution and cybersecurity corporations to trail and investigate the user deportment, making it simpler to detect individuals engaged in illegal activities.
- **Deepfake Technology**[45]**:** AI-generated deepfakes can be destroyed on the dark web to activate any misleading content, including fake news, identity theft, and fraudulent schemes. This technology further complicates the verification of information and can defame reputations or facilitate scams.

[43] Lavanya Elluri, Varun Mandalapu, Piyush Vyas & Nirmalya Roy, *Recent Advancements in Machine Learning for Cybercrime Prediction* (2023), arXiv Preprint arXiv:2304.04819, https://arxiv.org/abs/2304.04819 (last visited May 10, 2025).
[44] Kylie Foy, *Artificial Intelligence is Helping Investigators Fight Crime on the Dark Web*, MIT Lincoln Laboratory, https://www.ll.mit.edu/news/artificial-intelligence-helping-investigators-fight-crime-dark-web (last visited May 10, 2025)
[45] Robert Chesney & Danielle K. Citron, *Deep Fakes: A Looming Challenge for Privacy, Democracy, and National Security*, 107 Cal. L. Rev. 1753 (2019

- **Mechanical Scams and Fraud**[46]**:** AI algorithms can robotize the generations of scams, such as social engineering attacks and fake customer service interactions. These sophisticated schemes can deceive individuals more effectively than traditional methods.

IX. CASE STUDIES

A. AI Powered Phishing Attack

In 2019, Barracuda Networks[47] reported an increase in AI-powered phishing attacks, where machine learning algorithms were used to automate the creation of convincing phishing emails. These emails often mimicked legitimate communications, making them harder to detect.

AI-driven tools, particularly phishing simulations, used machine learning to analyze user behaviour and generate personalized phishing attacks. These tools could replicate website designs, email tones, and structure with high accuracy.

The primary legal concern was related to cybersecurity and data protection laws. The rise of AI-powered phishing necessitated stronger regulatory frameworks to protect individuals and organizations from these advanced cyber threats.

Barracuda Networks provided organizations with tools to better detect these sophisticated phishing attempts. As a result, law enforcement agencies began emphasizing the importance of AI tools in preventing cybercrimes, and companies were encouraged to adopt more robust cybersecurity measures.

[46] Marc Schmitt & Ivan Flechais, *Digital Deception: Generative Artificial Intelligence in Social Engineering and Phishing* (2023), arXiv Preprint arXiv:2310.13715, https://arxiv.org/abs/2310.13715 (last visited May 10, 2025)
[47] Barracuda Networks, *Business Email Compromise and AI-Driven Phishing Attacks: A New Era of Cyber Threats* (2019), https://www.barracuda.com/blog (last visited May 10, 2025).

B. AI Predective Policy[48] - MIT Technology Review[49]

Predictive policing algorithms, such as PredPol, were used by law enforcement agencies to predict crime hotspots and allocate resources. However, a study by MIT Technology Review found that these systems perpetuated racial biases, particularly against minority communities.

Predictive algorithms used historical crime data to forecast future crimes. However, these algorithms often relied on biased data, which led to discriminatory policing practices.

The legal concerns were centred around civil rights violations, particularly with regard to racial discrimination. The use of biased AI in policing raised questions about the ethical implications of automated decision-making in law enforcement.

The article highlighted the legal challenges faced by predictive policing systems, and several police departments were pressured to reform their use of AI tools. Discussions around the Accountability in AI Act gained traction, pushing for more oversight and fairness in AI-based law enforcement.

C. Autonomous AI Security System - Slack AI[50]

In 2023, a vulnerability in Slack AI allowed attackers to manipulate its features through prompt injection attacks, which exposed sensitive data stored in private channels.

Slack's AI-powered security features were compromised, enabling attackers to execute prompt injections that bypassed security protocols. These attacks exploited

[48] D. Will, *Artificial Intelligence: Predictive Policing Algorithms Are Racist. They Need to Be Dismantled*, MIT Tech. Rev. (2020)

[49] MIT Technology Review, *The Bias of AI in Predictive Policing and the Impact on Communities of Color* (2020), https://www.technologyreview.com/2020/02/18/91124/predictive-policing-ai-bias (last visited May 10, 2025)

[50] E. Montalbano, *Slack Patches AI Bug That Exposed Private Channels* (2024), Dark Reading, https://www.darkreading.com/cyberattacks-data-breaches/slack-ai-patches-bug-that-let-attackers-steal-data-from-private-channels (last visited May 10, 2025).

the AI's natural language processing capabilities, leading to unauthorized access to private information.

The incident raised concerns about data protection and privacy laws, especially under frameworks such as GDPR in Europe and the proposed Personal Data Protection Bill in India. Questions were raised about the accountability of AI developers in preventing such vulnerabilities.

Slack patched the vulnerability, and regulatory bodies began investigating the incident to determine if data protection regulations were violated. The case prompted organizations to reevaluate the use of AI in their security systems and adopt more stringent measures to ensure data privacy.

D. Case Study: Zomato Data Breach (2021) [51]

In 2021, Zomato, one of India's leading food delivery services, experienced a major data breach affecting millions of users. The breach was caused by a vulnerability in the company's AI-powered database system, which allowed unauthorized access to sensitive user data, including emails, phone numbers, and hashed passwords.

Zomato's AI-driven database system was responsible for storing user data. Hackers exploited vulnerabilities in the machine learning algorithms that managed access to this data. The breach raised significant concerns about how AI systems used by private companies could be targeted by cyberattacks, particularly in emerging markets like India.

The breach triggered discussions about data privacy laws in India, specifically in relation to the Personal Data Protection Bill (PDPB), which was still being debated in Parliament at the time. The incident raised questions about the adequacy of cybersecurity measures and the need for stronger regulation to safeguard user data.

In response to the breach, Zomato quickly took action to secure its systems and notified affected users. However, the breach became a case study for the Indian

[51] S. Nair, *Zomato Data Breach Exposes Millions of User Accounts: A Look at AI Vulnerabilities* (2021), The Economic Times, https://economictimes.indiatimes.com/technology/tech-bytes/zomato-data-breach-ai-vulnerabilities (last visited May 10, 2025).

government and regulatory bodies, pushing forward the adoption of stronger cybersecurity frameworks and more stringent data protection regulations. Additionally, the incident contributed to increasing awareness of the importance of securing AI-powered systems.

X. CONCLUSION

The emergence of Artificial Intelligence (AI) and its intersection with criminal liability in India presents complex and evolving challenges that require urgent attention from legal experts, policymakers, and AI developers. As AI technology advances, it increasingly plays a role in criminal offences, creating significant legal difficulties regarding liability, intention, and accountability. The lack of legal personhood for AI further complicates the criteria for assigning liability. Therefore, it is essential to address the accountability of AI developers, users, and operators through comprehensive legislative frameworks.

India's legal system must evolve proactively to accommodate the rapid development of AI technologies. The country's legislative framework needs to anticipate AI-driven challenges and develop dynamic laws that can adapt to technological advancements. The Personal Data Protection Bill (PDPB), along with the proposed AI regulations, should serve as foundational frameworks for addressing AI-related issues. Moving forward, India's laws will need to balance innovation with protection, ensuring that AI is used ethically and responsibly while safeguarding citizens' rights and privacy.

The concept of AI personhood, the question of intentionality in AI crimes, and the challenge of defining AI autonomy in criminal law will remain key areas for future legal research and development. This area of law is still in its infancy, and it is essential that India remains at the forefront of global discussions on AI ethics and liability.

XI. FUTURE RESEARCH DIRECTIONS

- **AI in Law Enforcement:** Research should focus on the implications of AI in policing, particularly around predictive policing, bias, and discrimination. Further studies could explore the development of AI transparency models that could be implemented in law enforcement and judicial proceedings.

- **Regulation of AI Algorithms:** As AI systems become more autonomous, research should delve into creating mechanisms for regulating AI algorithms, ensuring that they operate without causing harm to individuals or society. This could include the exploration of algorithmic accountability models and frameworks for ensuring fairness in automated decision-making.
- **International Collaboration and Legal Harmonization:** The global nature of AI technologies necessitates cross-border collaboration to harmonize AI regulations**.** Future research should explore international treaties or frameworks that ensure consistent standards for AI ethics, cybersecurity, and liability, especially in light of transnational cybercrimes.

By addressing these issues, India can build a robust legal framework that ensures the ethical and responsible use of AI, protecting both the interests of innovation and the rights of its citizens.

XII. REFERENCES

A. Books & Edited Volumes

- Chopra, S. and White, L.F., *A Legal Theory for Autonomous Artificial Agents* (University of Michigan Press 2011).
- Goodfellow, I., Bengio, Y. and Courville, A., *Deep Learning* (MIT Press 2016) 1–20.
- Martín, L.M. et al. (eds), *Artificial Intelligence and Human Rights* (Springer 2021).
- Brynjolfsson, E. and McAfee, A., *The Second Machine Age* (WW Norton 2014) 39–45.
- Russell, S. and Norvig, P., *Artificial Intelligence: A Modern Approach* (4th edn, Pearson 2020) 2–3.
- Pagallo, U., *The Laws of Robots: Crimes, Contracts, and Torts* (Springer 2013) 58–62, 117.
- Zuboff, S., *The Age of Surveillance Capitalism* (PublicAffairs 2019) 209–224.

- Amidei, C., Mazzotta, D.G. and Piñera, J., *Personhood and Artificial Intelligence* (Palgrave Macmillan 2021).

B. Journal Articles & SSRN Papers

- Cath, C. et al., 'Artificial Intelligence and the "Good Society"' (2018) 24 *Sci. & Eng'g Ethics* 505.
- Chesney, R. and Citron, D.K., 'Deep Fakes: A Looming Challenge for Privacy, Democracy, and National Security' (2019) 107 *Cal. L. Rev.* 1753.
- Bajpai, Y., 'Regulation of Risks Associated with Usage of Artificial Intelligence' (2024) 6 *Int'l J. Legal Sci. & Innovation* 13.
- Eggett, C., 'The Role of Principles in the Constitutional Processes of International Law' (2019) 66 *Neth. Int'l L. Rev.* 197.
- Taddeo, M. and Floridi, L., 'How AI Can Be a Force for Good' (2018) 361 *Science* 751.
- King, T.C. et al., 'Artificial Intelligence Crime: An Interdisciplinary Analysis' (2021) 27 & (2022) 28 *Sci. & Eng'g Ethics* 1.
- Seth, S., 'ML and AI: Interactions with the Right to Privacy' (2017) 52 *Econ. & Pol. Wkly.* 66.
- Sayyed, H., 'Artificial Intelligence and Criminal Liability in India' (2024) 10 *Cogent Soc. Sci.* 2343195.
- Kilara, A., 'Justification and Excuse under the IPC' (2007) 19 *Student B. Rev.* 12.
- Atrey, I., 'The Intersection of Artificial Intelligence and Law' (2023) https://ssrn.com/abstract=4632440.

C. Case Law

- M.C. Mehta v. Union of India (1987) 1 SCC 395.
- Anwar P.V. v. P.K. Basheer (2014) 10 SCC 473.

- Puttaswamy v. Union of India (2017) 10 SCC 1.

D. Preprints

- Kejriwal, M. et al., 'FlagIt: Human Trafficking Indicator Mining' (2017) arXiv:1712.03086.
- Elluri, L. et al., 'Machine Learning for Cybercrime Prediction' (2023) arXiv:2304.04819.
- Schmitt, M. and Flechais, I., 'Generative AI in Phishing' (2023) arXiv:2310.13715.

E. Government & Official Reports

- European Commission, *AI Act Proposal*, COM(2021) 206 final https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52021PC0206.
- Ministry of Education, *National Education Policy 2020* https://education.gov.in/....
- Ministry of Electronics & IT, *Digital India Act Discussion Paper* (2023) https://www.meity.gov.in.
- Nat'l Inst. of Justice, *Using AI to Address Criminal Justice Needs* (2018) https://www.ojp.gov/pdffiles1/nij/252038.pdf.
- U.S. Gov't Accountability Off., *AI: Emerging Challenges and Implications* (2021) https://www.gao.gov/products/gao-21-519sp.

F. News Articles & Media Reports

- Will, D., 'Predictive Policing Algorithms Are Racist' *MIT Tech. Rev.* (2020).
- MIT Technology Review, 'Bias of AI in Predictive Policing' (2020) https://www.technologyreview.com/....
- Foy, K., 'AI Helping Fight Crime on the Dark Web' *MIT Lincoln Lab* https://www.ll.mit.edu/news/....

- Kobie, N., 'China's AI Regulation' *Wired UK* (2022) https://www.wired.co.uk/....
- Chauriha, S., 'Digital India Act and Cyber Landscape' *The Hindu* (2023) https://www.thehindu.com.
- Barracuda Networks, *AI-Driven Phishing Attacks Report* (2019) https://www.barracuda.com/blog.
- Marwala, T., 'AI and the Law – Navigating the Future Together' (2024) *United Nations University* https://unu.edu/article/....
- Montalbano, E., 'Slack Patches AI Bug That Exposed Private Channels' (2024) *Dark Reading*, https://www.darkreading.com/cyberattacks-data-breaches/slack-ai-patches-bug-that-let-attackers-steal-data-from-private-channels (last visited May 10, 2025).
- Nair, S., 'Zomato Data Breach Exposes Millions of User Accounts: A Look at AI Vulnerabilities' (2021) *The Economic Times*, https://economictimes.indiatimes.com/technology/tech-bytes/zomato-data-breach-ai-vulnerabilities (last visited May 10, 2025).

G. Dictionaries & Reference Sites

- Oxford Advanced Learner's Dictionary (11th edn, 2010) https://www.oxfordlearnersdictionaries.com/ accessed 10 Jan 2025.
- Oxford Reference, 'Dark Web' https://www.oxfordreference.com/ accessed 10 May 2025.
- Legal Dictionary, 'Mens Rea Meaning in Law' https://www.law.cornell.edu/wex/mens_rea accessed 10 May 2025.