The Indian Journal for Research in Law and Management

Open Access Law Journal – Copyright © 2025
Editor-in-Chief – Dr. Muktai Deb Chavan; Publisher – Alden Vas; ISSN: 2583-9896

This is an Open Access article distributed under the terms of the Creative Commons Attribution-Non-Commercial-Share Alike 4.0 International (CC-BY-NC-SA 4.0) License, which permits unrestricted non-commercial use, distribution, and reproduction in any medium provided the original work is properly cited.

CRIME REDEFINED: HUMAN-AI INTERSECTION IN CYBERSPACE

~Nidh i Dadhich

❖ INTRODUCTION

The digital revolution has transformed every facet of modern life, and nowhere is this more evident than in the realm of crime. Artificial intelligence (AI) is rapidly reshaping the landscape of cyberspace, introducing new opportunities and unprecedented threats. The intersection of human behaviour and AI technology is redefining what crime looks like, how it is perpetrated, and how society responds. This article explores the evolving nature of cybercrime from legal and criminal psychology perspectives, highlighting the challenges and opportunities presented by AI. By analysing current trends, legal frameworks, and psychological dynamics, we aim to provide a nuanced understanding of crime in the age of AI[1].

❖ THE EVOLUTION OF CRIME IN THE DIGITAL AGE

Historically, crime was largely defined by physical acts—theft, assault, and fraud carried out in the tangible world. The advent of the internet introduced cybercrime, a category that includes hacking, identity theft, and online scams[2]. However, the rise of AI has ushered in a new era of criminal activity. Offenders now leverage machine learning, natural language processing, and automation to perpetrate crimes at a scale and sophistication previously unimaginable.[3]

---

[1] Amit Kumar & Priya Sharma, Artificial Intelligence and Cyber Laws in India: A Legal Perspective, 13 Int'l J. Sci. & Tech. 16 (2025), https://www.ijsat.org/papers/2025/1/1316.pdf; Anirudh Rastogi & Anshuman Sakle, India, in Cybersecurity Laws and Regulations 2025, Int'l Comp. Legal Guides, https://iclg.com/practice-areas/cybersecurity-laws-and-regulations/india (last visited June 24, 2025).

[2]Cyber Laws and Recent Developments, Khurana & Khurana (Feb. 21, 2025), https://www.khuranaandkhurana.com/2025/02/21/cyber-laws-and-recent-developments/. (last visited June 25, 2025)

[3] See Amit Kumar & Priya Sharma, Artificial Intelligence and Cyber Laws in India: A Legal Perspective, supra note 1.

Early cybercrimes were often opportunistic, relying on manual effort and limited technical skill. Today, AI enables criminals to automate attacks, personalize scams, and evade detection with greater efficiency.[4] For example, phishing emails have evolved from generic messages to highly targeted campaigns crafted by AI algorithms that analyse victims' online behaviour. Deepfakes—AI-generated videos and audio—are being used to impersonate individuals, manipulate public opinion, and commit fraud[5]. These developments signify a fundamental shift in the nature of crime, driven by the convergence of human ingenuity and machine intelligence.

❖ CRIMINAL PSYCHOLOGY AND AI: NEW MOTIVATIONS AND BEHAVIOURS

Understanding the motivations behind AI-enabled cybercrime requires a deep dive into criminal psychology. Traditional theories of crime, such as routine activity theory, remain relevant but must be adapted to the digital context. Routine activity theory posits that crime occurs when a motivated offender, a suitable target, and the absence of a capable guardian converge. In cyberspace, AI lowers barriers to entry for offenders, making it easier for individuals with limited technical expertise to engage in sophisticated criminal activities.

The psychological motivations for cybercrime are diverse. Some offenders are driven by financial gain, while others seek power, recognition, or the thrill of outsmarting security systems[6]. The anonymity afforded by the internet emboldens individuals to take risks they might avoid in the physical world[7]. AI amplifies these tendencies by enabling offenders to automate attacks, scale their operations, and personalize their approaches.

Social engineering, a tactic that exploits human psychology to gain access to sensitive information, has become more potent with AI. Machine learning algorithms can analyse vast amounts of data to craft highly persuasive messages tailored to individual victims. This level

[4] See generally Anirudh Rastogi & Anshuman Sakle, supra note 1.

[5] See generally Press Information Bureau, Government of India, PIB's Fact Check Unit Issues Advisory Against Deepfakes (Apr. 24, 2025), https://www.pib.gov.in/PressReleasePage.aspx?PRID=2119050.

[6] Psychological Profiling in Cybersecurity: A Look at LLMs and Human Factors, arXiv (May 12, 2024), https://arxiv.org/html/2406.18783v1. (last visited June, 26 2025)

[7] Hacking the Mind: Why Psychology Matters to Cybersecurity, IBM (Feb. 6, 2025), https://www.ibm.com/think/insights/hacking-the-mind-why-psychology-matters-to-cybersecurity.

of personalization increases the likelihood of success, as victims are more likely to trust messages that appear legitimate and relevant to their interests.[89]

❖ LEGAL FRAMEWORKS AND CHALLENGES

The rapid evolution of AI-enabled cybercrime has outpaced the development of legal frameworks designed to address it. Most countries have established laws to combat cybercrime, such as the Computer Fraud and Abuse Act in the United States and the Cybercrime Prevention Act in the Philippines. However, these laws were drafted before the widespread adoption of AI and often fail to address the unique challenges posed by intelligent systems.[10]

One of the most significant legal challenges is attributing responsibility for AI-facilitated crimes. When an AI system is used to commit a crime, determining who is liable—the developer, the user, or the AI itself can be complex. Legal doctrines such as mens rea (criminal intent) become muddled when actions are automated or semi-autonomous. Jurisdictional issues further complicate matters, as cybercrime often transcends national borders, making enforcement and prosecution difficult.

Emerging legal doctrines are beginning to address these challenges. Some jurisdictions are exploring the concept of "algorithmic accountability," which holds developers and users responsible for the actions of their AI systems. However, much work remains to be done to ensure that legal frameworks keep pace with technological advancements.[11]

India's primary legal instrument for cybercrimes is the **Information Technology Act, 2000 (IT Act)**, which criminalizes unauthorized access, data theft, hacking, and tampering with computer source documents (Sections 43, 65, 66, etc.)[12][13]. The **Digital Personal Data**

[8] The Psychology Behind Cyber Attacks: Understanding the Attacker, Global Cybersecurity Network, https://globalcybersecuritynetwork.com/blog/the-psychology-behind-cyber-attacks/ (Last visited June 25, 2025)

[9] Arunesh Bal, The Psychology of Cyber Fraud: How Scammers Use AI to Exploit Human Behaviour, Int'l J. Creative Res. Thoughts, Vol. 12, Issue 7, 2024, https://ijcrt.org/papers/IJCRT2407696 (last Visited, June 26, 2025).

[10] AI and Serious Online Crime, The Alan Turing Institute, https://cetas.turing.ac.uk/publications/ai-and-serious-online-crime, (last visited June 25, 2025).

[11] Ibid.

[12] Information Technology Act, 2000, § 43, 65, 66 (India)

[13] See, Amit Kumar & Priya Sharma, Artificial Intelligence and Cyber Laws in India: A Legal Perspective, 13 Int'l J. Sci. & Tech. 16 (2025), Supra note 1.

Protection Act, 2023 (DPDP Act)[14] was enacted to address data privacy and protection in the digital era[15]. These laws, supplemented by sectoral regulations and guidelines, form the backbone of India's cyber legal framework.

➢ KEY LEGAL PROVISIONS:

- Section 65, IT Act: Punishes tampering with computer source documents with imprisonment up to three years or a fine, or both[16].
- Section 66, IT Act: Addresses computer-related offences, including hacking and unauthorized access.
- Section 66C & 66D, IT Act: Deal with identity theft and cheating by personation using computer resources.
- DPDP Act, 2023: Regulates the processing of digital personal data, aiming to protect privacy and impose obligations on data fiduciaries[17][18]

➢ RECENT POLICY INITIATIVES:

- The Government of India has clarified that the IT Act and its rules apply to information generated using AI tools, including deepfakes and synthetic media. Also, Law enforcement is being trained in AI detection software to track and investigate cybercrimes involving AI-generated content[19].

➢ INCONSISTENCIES AND CHALLENGES:

[14] Digital Personal Data Protection Act, 2023 (India)

[15] See, Cyber Laws and Recent Developments, Khurana & Khurana (Feb. 21, 2025), Supra note 2.

[16] See, Anirudh Rastogi & Anshuman Sakle, India, in Cybersecurity Laws and Regulations 2025, Int'l Comp. Legal

, Supra Note, 1

[17] See, Cyber Laws and Recent Developments, Khurana & Khurana (Feb. 21, 2025), Supra note 2.

[18] See, Press Information Bureau, Government of India, PIB's Fact Check Unit Issues Advisory Against Deepfakes (Apr. 24, 2025), Supra note 5.

[19] Bharatiya Laws Against Deepfake Cybercrime: Opportunities and Challenges, Vivekananda Int'l Found. (Apr. 28,2025), https://www.vifindia.org/article/2025/april/28/Bharatiya-Laws-Against-Deepfake-Cybercrime-Opportunities-and-Challenges, (last visited June, 23 2025).

- Lack of AI-Specific Provisions: The IT Act does not explicitly address crimes committed using or by AI systems, leading to ambiguity in attribution of liability (e.g., whether the developer, deployer, or user is responsible for AI-generated harm)[20].
- Jurisdictional Issues: Cybercrimes involving AI often cross-national borders, complicating investigation and prosecution due to varying international standards and cooperation mechanisms.
- Enforcement and Capacity Gaps: Law enforcement agencies often lack the technical expertise and resources to investigate sophisticated AI-driven crimes, such as deepfake fraud or automated phishing attacks[21].

➢ **PRIVACY AND SURVEILLANCE CONCERNS:**

- The increased use of AI for surveillance and crime detection raises concerns about mass surveillance and potential violations of privacy rights under Article 21 of the Indian Constitution[22].
- Rapid Technological Evolution: The legal system struggles to keep pace with the speed at which AI technologies evolve, resulting in outdated laws and regulatory lag.

❖ **CASE STUDIES: HUMAN-AI COLLABORATION IN CRIME**

Several high-profile cases illustrate the growing collaboration between humans and AI in criminal activities. Deepfake technology, for example, has been used to create convincing videos of public figures saying or doing things they never did. These videos have been deployed in fraud schemes, political disinformation campaigns, and even blackmail. In one notable case, a CEO was tricked into transferring millions of dollars after receiving a phone call from what sounded like his boss- a voice generated by AI[23].

AI-powered social engineering is another area of concern. Phishing campaigns now use machine learning to analyse social media profiles and craft messages that are highly personalized and difficult to distinguish from legitimate communications. Tech support scams

[20] See, Amit Kumar & Priya Sharma, Artificial Intelligence and Cyber Laws in India: A Legal Perspective, 13 Int'l J. Sci. & Tech. 16 (2025), Supra note 1.

[21] Supra Note 19.

[22] India Const. art. 21.

[23] See, Bharatiya Laws Against Deepfake Cybercrime: Opportunities and Challenges, Vivekananda Int'l Found. (Apr. 28, 2025), Supra note, 19.

have also become more sophisticated, with AI chatbots impersonating customer service representatives to extract sensitive information from victims.[24]

The arms race between criminal and legal AI tools is intensifying. Law enforcement agencies are increasingly adopting AI to detect and prevent cybercrime, but criminals are also using AI to evade detection. This dynamic underscore the need for ongoing innovation and collaboration among legal, technological, and psychological experts.

❖ CRIMINAL JUSTICE RESPONSE AND ETHICAL CONSIDERATIONS

Law enforcement agencies are adapting to the challenges posed by AI-enabled cybercrime by integrating AI into their investigative and preventive efforts. AI tools can analyse vast datasets to identify patterns, predict potential threats, and automate routine tasks. For example, machine learning algorithms can flag suspicious transactions, detect anomalies in network traffic, and identify potential victims of fraud[25].

However, the use of AI in law enforcement raises important ethical considerations. Privacy concerns are paramount, as the collection and analysis of large datasets can infringe on individuals' rights. Bias in AI algorithms is another critical issue; if not properly designed, AI systems can perpetuate or exacerbate existing inequalities. For instance, facial recognition technology has been criticized for its higher error rates among certain demographic groups.[26]

Professional and regulatory guidelines are essential to ensure the responsible use of AI in criminal justice. Organizations such as the European Union's General Data Protection Regulation (GDPR) and the Algorithmic Accountability Act in the United States are steps in the right direction, but more comprehensive frameworks are needed to address the unique challenges of AI-enabled crime.[27]

---

[24] See generally, Press Information Bureau, Government of India, PIB's Fact Check Unit Issues Advisory Against Deepfakes (Apr. 24, 2025), Supra note, 5.

[25] See, Amit Kumar & Priya Sharma, *Artificial Intelligence and Cyber Laws in India: A Legal Perspective*, 13 Int'l J. Sci. & Tech. 16, 22–23 (2025), Supra Note 1.

[26] See, Anirudh Rastogi & Anshuman Sakle, *India*, in Cybersecurity Laws and Regulations 2025, Int'l Comp. Legal Guides, Supra note 1.

[27] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation), 2016 O.J. (L 119) 1; Algorithmic Accountability Act of 2022, H.R. 6580, 117th Cong. (2022).

❖ CONCLUSION & FUTURE DIRECTIONS: POLICY, PREVENTION, AND PSYCHOLOGY

Looking ahead, policymakers, researchers, and practitioners must work together to address the evolving threat landscape. Strengthening legal frameworks to keep pace with technological advancements is a top priority. International cooperation is essential to combat cross-border cybercrime and ensure consistent enforcement.[28]

Preventive measures should focus on public awareness, education, and technological safeguards. Educating individuals about the risks of AI-enabled scams and promoting cybersecurity best practices can reduce vulnerability. Technological solutions, such as advanced encryption and AI-driven threat detection, can help protect sensitive data and systems.[29]

Criminal psychology research must also evolve to understand the changing profiles of offenders and victims. By studying the motivations, behaviours, and decision-making processes of cybercriminals, researchers can develop more effective strategies for prevention and intervention.

The intersection of human behaviour and AI in cyberspace is redefining the nature of crime and challenging traditional legal and psychological frameworks. AI-enabled cybercrime presents new risks and complexities, but also opportunities for innovation in detection, prevention, and response. Addressing these challenges requires interdisciplinary collaboration among legal experts, psychologists, technologists, and policymakers. By balancing innovation with security and justice, society can harness the benefits of AI while mitigating its risks. The future of crime prevention lies in our ability to adapt, collaborate, and remain vigilant in the face of ever-evolving threats.

❖ REFERENCES

➢ LEGISLATION

- Digital Personal Data Protection Act, 2023 (India).
- Information Technology Act, 2000, §§ 43, 65, 66 & 67 (India).

[28] See, Amit Kumar & Priya Sharma, *Artificial Intelligence and Cyber Laws in India: A Legal Perspective*, 13 Int'l J. Sci. & Tech. 16, 22–23 (2025), Supra Note 1.

[29] See, Press Information Bureau, Government of India, PIB's Fact Check Unit Issues Advisory Against Deepfakes, Supra note, 5.

➢ CONSTITUTIONAL PROVISIONS

- India Const. art. 21.

➢ INTERNATIONAL INSTRUMENTS

- Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation), 2016 O.J. (L 119) 1.
- Algorithmic Accountability Act of 2022, H.R. 6580, 117th Cong. (2022).

➢ BOOKS, JOURNAL ARTICLES, AND LAW REVIEWS

- Amit Kumar & Priya Sharma, Artificial Intelligence and Cyber Laws in India: A Legal Perspective, 13 Int'l J. Sci. & Tech. 16 (2025), https://www.ijsat.org/papers/2025/1/1316.pdf.
- Anirudh Rastogi & Anshuman Sakle, India, in Cybersecurity Laws and Regulations 2025, Int'l Comp. Legal Guides, https://iclg.com/practice-areas/cybersecurity-laws-and-regulations/india
- Arunesh Bal, The Psychology of Cyber Fraud: How Scammers Use AI to Exploit Human Behaviour, Int'l J. Creative Res. Thoughts, Vol. 12, Issue 7, 2024, https://ijcrt.org/papers/IJCRT2407696.pdf

➢ REPORTS, WEBSITES, AND OTHER SECONDARY SOURCES

- AI and Serious Online Crime, The Alan Turing Institute, https://cetas.turing.ac.uk/publications/ai-and-serious-online-crime
- Bharatiya Laws Against Deepfake Cybercrime: Opportunities and Challenges, Vivekananda Int'l Found. (Apr. 28, 2025), https://www.vifindia.org/article/2025/april/28/Bharatiya-Laws-Against-Deepfake-Cybercrime-Opportunities-and-Challenges
- Cyber Laws and Recent Developments, Khurana & Khurana (Feb. 21, 2025), https://www.khuranaandkhurana.com/2025/02/21/cyber-laws-and-recent-developments/
- Hacking the Mind: Why Psychology Matters to Cybersecurity, IBM (Feb. 6, 2025), https://www.ibm.com/think/insights/hacking-the-mind-why-psychology-matters-to-cybersecurity.
- Press Information Bureau, Government of India, PIB's Fact Check Unit Issues Advisory Against Deepfakes (Apr. 24, 2025), https://www.pib.gov.in/PressReleasePage.aspx?PRID=2119050

- Psychological Profiling in Cybersecurity: A Look at LLMs and Human Factors, arXiv (May 12, 2024), https://arxiv.org/html/2406.18783v1
- The Psychology Behind Cyber Attacks: Understanding the Attacker, Global Cybersecurity Network, https://globalcybersecuritynetwork.com/blog/the-psychology-behind-cyber-attacks/