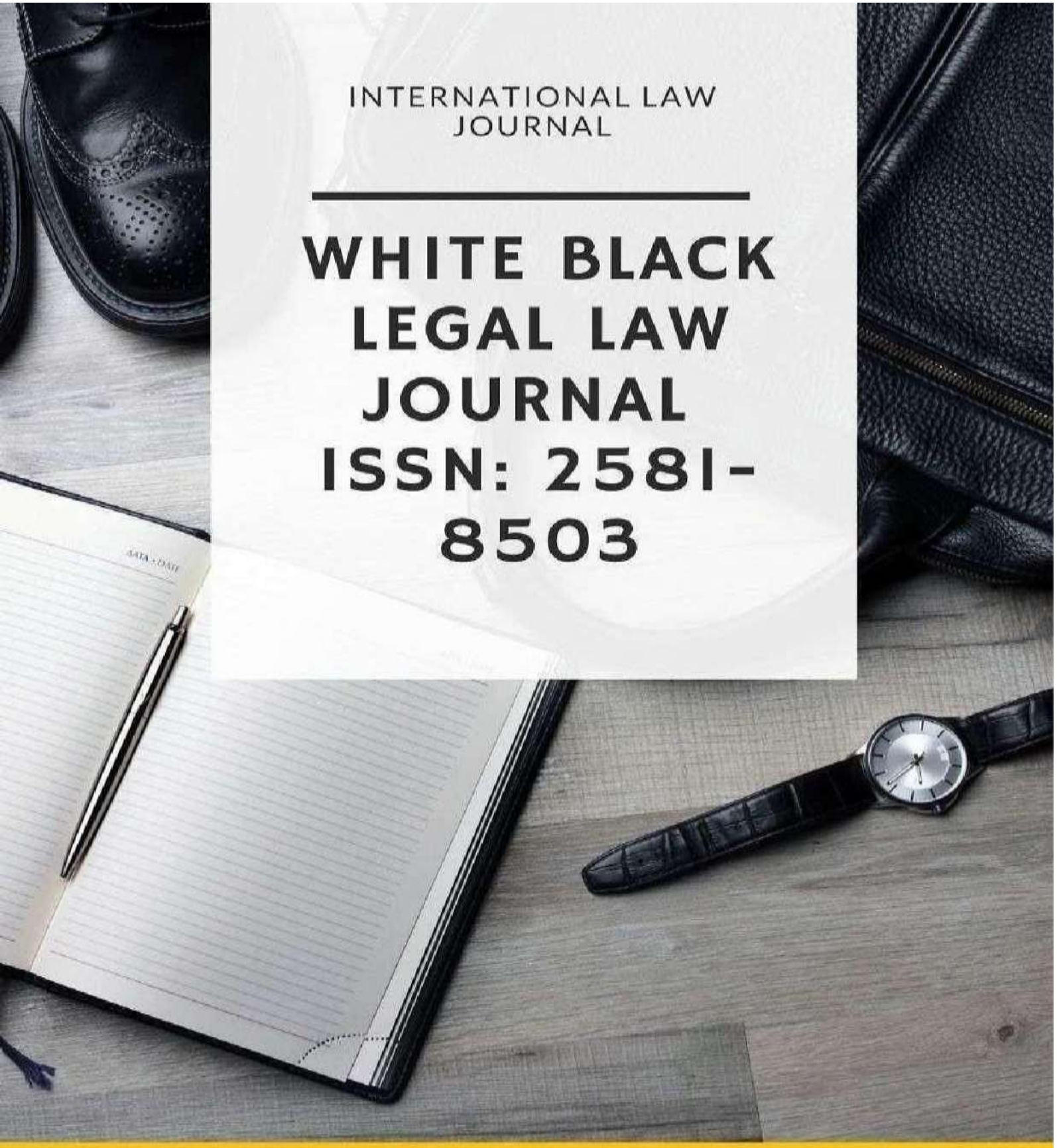

INTERNATIONAL LAW JOURNAL

WHITE BLACK LEGAL LAW JOURNAL

ISSN: 2581-8503

Peer - Reviewed & Refereed Journal

The Law Journal strives to provide a platform for discussion of International as well as National Developments in the Field of Law.

DISCLAIMER

ABOUT WHITE BLACK LEGAL

White Black Legal – The Law Journal is an open-access, peer-reviewed, and refereed legal journal established to provide a scholarly platform for the examination and discussion of contemporary legal issues. The journal is dedicated to encouraging rigorous legal research, critical analysis, and informed academic discourse across diverse fields of law.

The journal invites contributions from law students, researchers, academicians, legal practitioners, and policy scholars. By facilitating engagement between emerging scholars and experienced legal professionals, *White Black Legal* seeks to bridge theoretical legal research with practical, institutional, and societal perspectives.

In a rapidly evolving social, economic, and technological environment, the journal endeavours to examine the changing role of law and its impact on governance, justice systems, and society. *White Black Legal* remains committed to academic integrity, ethical research practices, and the dissemination of accessible legal scholarship to a global readership.

AIM & SCOPE

The aim of *White Black Legal – The Law Journal* is to promote excellence in legal research and to provide a credible academic forum for the analysis, discussion, and advancement of contemporary legal issues. The journal encourages original, analytical, and well-researched contributions that add substantive value to legal scholarship.

The journal publishes scholarly works examining doctrinal, theoretical, empirical, and interdisciplinary perspectives of law. Submissions are welcomed from academicians, legal professionals, researchers, scholars, and students who demonstrate intellectual rigour, analytical clarity, and relevance to current legal and policy developments.

The scope of the journal includes, but is not limited to:

- Constitutional and Administrative Law
- Criminal Law and Criminal Justice
- Corporate, Commercial, and Business Laws
- Intellectual Property and Technology Law
- International Law and Human Rights
- Environmental and Sustainable Development Law
- Cyber Law, Artificial Intelligence, and Emerging Technologies
- Family Law, Labour Law, and Social Justice Studies

The journal accepts original research articles, case comments, legislative and policy analyses, book reviews, and interdisciplinary studies addressing legal issues at national and international levels. All submissions are subject to a rigorous double-blind peer-review process to ensure academic quality, originality, and relevance.

Through its publications, *White Black Legal – The Law Journal* seeks to foster critical legal thinking and contribute to the development of law as an instrument of justice, governance, and social progress, while expressly disclaiming responsibility for the application or misuse of published content.

WHITE COLLAR CRIME AND ARTIFICIAL INTELLIGENCE: EMERGING THREATS, ENABLERS AND THE REGULATORY IMPERATIVE

AUTHORED BY - BHAKTI TALATHI
LL.M. Programme
Vishvakarma University

ABSTRACT

The intersection of artificial intelligence (AI) and white-collar crime represents one of the most consequential and under-theorised challenges facing contemporary criminal law and corporate regulation. White collar crime a concept first systematically articulated by Edwin Sutherland in 1949 as crime committed by a person of respectability and high social status in the course of his occupation has undergone a profound technological metamorphosis in the twenty-first century.[1] AI-powered tools are simultaneously serving as instruments of sophisticated financial fraud, market manipulation, identity theft and money laundering, while also offering regulators and compliance professionals novel means of detection and prevention. This article examines the dual character of AI in white collar criminality: first, as an enabler of new and amplified forms of financial wrongdoing; second, as a tool for law enforcement and regulatory bodies. It further surveys the current legislative landscape in India and internationally, identifies critical lacunae, and proposes a coherent regulatory framework adequate to the AI era.[2]

Keywords: White Collar Crime, Artificial Intelligence, Financial Fraud, Market Manipulation, Deepfakes, Algorithmic Collusion, Regulatory Framework, India.

I. INTRODUCTION

White collar crime has long occupied an uncomfortable position within criminological discourse: recognised as deeply harmful to economic order and public trust, yet persistently under-prosecuted and inadequately theorised. The traditional image of the white collar criminal the company director, the corrupt banker, the insider trader has been complicated beyond recognition by the advent of artificial intelligence. Crimes that once required sophisticated human expertise and elaborate human networks can now be executed at scale,

speed and anonymity that existing legal instruments were never designed to address.

The scale of the problem is considerable. Europol's Internet Organised Crime Threat Assessment for 2023 identified AI-assisted fraud as one of the fastest-growing categories of financial crime in the European Union.[3] The United States Federal Bureau of Investigation reported losses of over USD 12.5 billion attributable to internet-based white collar crimes in 2023, a figure representing a significant acceleration from prior years.[4]

PricewaterhouseCoopers' Global Economic Crime Survey of 2022 found that 46 per cent of organisations globally reported experiencing fraud, corruption or other economic crime, with AI-related fraud emerging as a prominent sub-category.[5]

India presents a particularly compelling case study. The country's rapid digitalisation spanning banking, securities markets, insurance, taxation and public procurement has vastly enlarged the attack surface for technologically sophisticated white collar criminals, while regulatory and enforcement institutions are still in the process of acquiring the tools and expertise necessary to respond.[6] This article proceeds in five substantive parts: an examination of the conceptual relationship between AI and white collar crime; an account of the principal modalities of AI-enabled financial wrongdoing; an analysis of AI as a detection mechanism; a survey of the regulatory landscape; and a set of reform proposals.

II. CONCEPTUAL FRAMEWORK: AI AND THE ANATOMY OF WHITE-COLLAR CRIME

2.1 Definitional Contours

White collar crime, as codified in Indian law across statutes such as the Prevention of Money Laundering Act 2002, the Securities and Exchange Board of India Act 1992, and the Companies Act 2013, encompasses a wide range of non-violent, financially motivated offences committed by individuals or entities occupying positions of trust or authority.[7][8] The defining characteristics breach of trust, concealment, financial motivation, and exploitation of institutional position are each affected in distinctive ways by AI-enabled tools and techniques.[9]

2.2 AI as a Force Multiplier

AI alters the economics of white-collar crime in three fundamental respects. First, it dramatically reduces the cost and expertise required to execute complex fraudulent schemes. Tasks that previously required skilled accountants, lawyers or traders producing convincing forged documents, identifying patterns of regulatory arbitrage, executing precisely timed

market trades can now be automated and run at scale. Second, AI enhances the concealment capacity of white-collar criminals, enabling them to generate synthetic identities, fabricate digital evidence and launder proceeds through complex transactional chains that are difficult to trace. Third, AI radically accelerates the tempo of financial crime, compressing the window within which investigators and regulators might detect and interdict wrongdoing.[1011]

The Financial Stability Board has noted that AI and machine learning tools, while created for legitimate financial purposes, carry inherent dual-use risks that financial regulators have been slow to address.[12] Ryder has observed that the application of advanced technology to financial crime has created what might be described as an asymmetric threat landscape, in which criminal actors are frequently better equipped than those tasked with combating them.[13]

III. MODALITIES OF AI-ENABLED WHITE-COLLAR CRIME

3.1 Deepfake-Based Fraud and Identity Deception

Deepfakes AI-generated synthetic media that convincingly replicate the appearance and voice of real individuals represent perhaps the most viscerally alarming application of AI to white collar crime. Europol has documented a growing category of fraud in which deepfake audio and video of corporate executives are used to authorise fraudulent wire transfers, often bypassing institutional verification protocols that were not designed to authenticate digital media.[14] The underlying technology, based on generative adversarial networks and diffusion models, has advanced to the point where real-time deepfake generation is feasible on consumer hardware, dramatically lowering barriers to access.[15]

The Federal Trade Commission in the United States recorded a significant increase in AI voice-cloning scams in 2023, in which criminals replicated the voices of family members, corporate officers or government officials to induce fraudulent payments.[16] In the Indian context, several high-profile cases have involved the use of morphed video to facilitate corporate identity fraud and to manipulate potential investors, though domestic legislation principally the Information Technology Act 2000 and its amendments does not specifically address the production or deployment of deepfakes for fraudulent purposes.[31]

3.2 AI-Driven Market Manipulation

Securities markets have always been vulnerable to manipulation, but AI-powered tools have introduced qualitatively new threats. Algorithmic trading systems, when deployed with manipulative intent, can execute layering and spoofing strategies placing and cancelling large

orders to create artificial price signals at speeds and volumes that far exceed the capacity of human-operated market surveillance systems.[24] Sentiment analysis algorithms, trained on social media feeds and news aggregators, can be weaponised to identify market vulnerabilities and coordinate artificial price movements timed to coincide with engineered information events.[25]

The Securities and Exchange Board of India has recognised algorithmic trading as a source of systemic risk and introduced the SEBI Circular on Algorithmic Trading of 2012, subsequently revised, which mandates risk controls and audit trails for algorithmic trading systems.[8] However, the current regulatory framework does not specifically address the use of AI to construct self-optimising market manipulation strategies that adapt in real time to regulatory countermeasures, a gap that represents a pressing legislative priority.[20]

3.3 AI-Assisted Money Laundering

Money laundering the process of concealing the illicit origin of criminal proceeds has been substantially enhanced by AI. Machine learning models can identify patterns in financial regulations across jurisdictions to find optimal layering strategies, automating the placement of funds through cascades of shell entities, cryptocurrencies and trade finance instruments that are highly difficult for conventional anti-money laundering (AML) systems to detect.[722] AI-powered tools can also analyse the behavioural patterns of AML monitoring systems and route transactions to avoid triggering threshold-based alerts, a phenomenon known as adversarial evasion.[23]

India's Financial Intelligence Unit has noted increasing complexity in money laundering typologies linked to digital payment platforms, cryptocurrency exchanges and cross-border remittance systems, all of which are potential vectors for AI-assisted laundering.[27] The Prevention of Money Laundering Act 2002, while regularly amended, was not designed with AI-enabled layering in mind and contains no provisions specifically addressing the use of automated systems to structure transactions in evasion of reporting obligations.[7]

3.4 Algorithmic Collusion and Antitrust Violations

Algorithmic collusion in which pricing algorithms operated by competing firms converge on supercompetitive prices without any direct communication between their operators poses profound challenges for competition law. Because the collusion emerges from the independent operation of algorithmic systems rather than from explicit agreement, it may fall outside the scope of prohibitions on concerted practices that require proof of a meeting of minds.[2021] Tim

Wu has argued that the concentration of AI capabilities within a small number of dominant platforms creates conditions highly conducive to algorithmic rent-seeking that competition law has not yet adequately theorised.[35]

The Competition Commission of India's market study on e-commerce, published in 2020, identified algorithmic pricing as a significant risk to market competition but stopped short of recommending specific legislative intervention.[21] The subsequent Competition (Amendment) Act 2023 introduced provisions relating to digital markets, though the adequacy of these provisions to address AI-driven collusion remains a matter of active scholarly debate.[20]

3.5 Data Harvesting and Privacy-Based White-Collar Offences

The commercial harvesting of personal data through AI systems, in violation of privacy law and fiduciary obligations, constitutes an emerging category of white -collar offending. Zuboff's theory of surveillance capitalism provides a powerful analytical frame: corporations systematically extract behavioural data from consumers, process it through AI systems to generate predictive models of human behaviour, and deploy those models in ways that were never consented to and that cause diffuse but serious social harm.[17] Yanisky-Ravid and Hallisey have argued for a model of AI data transparency through audit and certification regimes as a means of converting diffuse harms into cognisable legal violations.[18]

In India, the Digital Personal Data Protection Act 2023 represents the primary legislative response to data misuse, creating obligations of notice, consent and purpose limitation that are potentially applicable to AI systems processing personal data for commercial gain.[32] However, significant enforcement challenges remain, particularly with respect to attributing responsibility for AI-driven data processing to identifiable corporate actors.[30]

IV. AI AS A TOOL FOR DETECTION AND PREVENTION

4.1 Machine Learning in Anti-Money Laundering

The same capabilities that make AI a potent instrument of financial crime also make it a powerful tool for its detection. Machine learning models, trained on large datasets of historical financial transactions, can identify anomalous patterns indicative of money laundering, fraud or insider trading with a degree of sensitivity and specificity that substantially exceeds rule-based monitoring systems.[2223] KPMG's analysis of AML applications found that AI-powered transaction monitoring systems reduced false positive rates by up to 70 per cent compared to conventional rule-based systems, significantly improving the efficiency of compliance

operations.[22]

4.2 Network Analysis and Beneficial Ownership

Graph-based AI systems capable of analysing complex networks of corporate relationships have proven particularly valuable in identifying the beneficial ownership structures used to conceal illicit assets. By mapping relationships across corporate registries, land records, financial disclosures and public databases, AI systems can construct ownership maps that would take human investigators months to assemble, and can do so continuously and at scale.[39] INTERPOL has reported substantial successes using AI-powered network analysis tools to identify beneficial ownership patterns in major cross-border corruption investigations.[38]

4.3 Forensic Audit and AI

Forensic auditing, which plays a central role in the investigation of corporate fraud under the Companies Act 2013 and the Insolvency and Bankruptcy Code 2016, has been substantially enhanced by AI-powered document analysis tools. These systems can process millions of pages of corporate records, emails and financial statements to identify discrepancies, irregular patterns and potentially fraudulent entries far more rapidly than human auditors.[37] The Serious Fraud Investigation Office has begun integrating AI-assisted forensic tools into its investigative methodology, though resource constraints and data access limitations remain significant obstacles.[37]

4.4 Challenges and Limitations

The deployment of AI in law enforcement and regulatory contexts raises significant concerns that must not be overlooked. AI detection systems can themselves be compromised through adversarial manipulation, in which criminal actors deliberately craft transactions or documents to evade algorithmic detection. The opacity of complex machine learning models creates evidentiary challenges in criminal proceedings, where the reliability of AI-generated evidence may be contested.[19] Furthermore, the concentration of advanced AI capabilities in large commercial providers creates dependency relationships that raise questions about data sovereignty and investigative integrity, concerns that are particularly acute in the Indian context.[26]

V. REGULATORY LANDSCAPE: INDIA AND INTERNATIONAL

COMPARISONS

5.1 The Indian Framework

India's regulatory response to AI-facilitated white-collar crime remains fragmented across multiple legislative instruments, none of which was specifically designed with AI in mind. The principal statutes — the Indian Penal Code 1860 (now the Bharatiya Nyaya Sanhita 2023), the Information Technology Act 2000, the Prevention of Money Laundering Act 2002, the SEBI Act 1992, the Companies Act 2013 and the Digital Personal Data Protection Act 2023 collectively provide a partial but ultimately inadequate foundation for addressing AI-enabled financial wrongdoing.[319]

The Reserve Bank of India has taken an increasingly proactive approach to AI-related financial risks, issuing guidelines on the use of AI in lending, payments and fraud prevention through a series of circulars and the Working Group Report on Digital Lending of 2021.[27] SEBI has similarly issued circulars on algorithmic trading and cybersecurity, and has established a dedicated Technology Advisory Committee. However, these regulatory responses have been primarily oriented toward systemic risk management rather than the criminalisation of AI-facilitated misconduct.[8]

NITI Aayog's National Strategy for Artificial Intelligence of 2018, while articulating a vision of responsible AI development, does not contain provisions specifically addressing the criminal misuse of AI in financial contexts, and there is no dedicated AI regulation in force in India as of 2025.[26] The Central Bureau of Investigation and the Enforcement Directorate have developed specialised cyber forensics capabilities, but their capacity to investigate AI-specific white collar offences remains limited.[33]

5.2 International Regulatory Approaches

The European Union's Artificial Intelligence Act 2024 the world's first comprehensive statutory framework for AI regulation establishes a risk-based classification system under which AI applications in critical sectors, including financial services, are subject to heightened conformity assessments, transparency obligations and human oversight requirements.[28] While the AI Act is primarily a product safety and fundamental rights instrument rather than a criminal law statute, its transparency and accountability requirements create a normative infrastructure that is directly relevant to the prevention of AI-facilitated financial misconduct.[28]

The United States has adopted a more sectoral approach, with the Securities and Exchange Commission, the Financial Industry Regulatory Authority and the Department of Justice each

pursuing AI-related enforcement actions within their respective jurisdictions. The SEC's enforcement action against an algorithmic trading firm for AI-assisted market manipulation in 2023 represented a landmark application of existing market manipulation prohibitions to AI-powered trading strategies.[24] The Financial Action Task Force has issued guidance on the application of anti-money laundering standards to virtual assets and AI-enabled financial services, though this guidance is non-binding and has been adopted unevenly across member jurisdictions.[38]

VI. REFORM PROPOSALS AND RECOMMENDATIONS

The preceding analysis suggests that the current regulatory architecture in India and internationally is inadequate to address the challenge of AI-enabled white-collar crime in a systematic and effective manner. The following reforms are proposed.

First, India should enact a dedicated Artificial Intelligence (Regulation of High-Risk Applications) Act, modelled in part on the EU AI Act, that subjects AI systems used in financial services, insurance, credit assessment and market trading to mandatory conformity assessments, transparency obligations and human oversight requirements. The Act should include specific provisions creating liability criminal as well as civil for the deployment of AI systems with knowledge or reckless disregard of their use in facilitating financial crime.[2830]

Second, the Prevention of Money Laundering Act 2002 should be amended to expressly address AI-assisted layering and placement strategies, including provisions requiring financial institutions to deploy AI-based transaction monitoring systems that are regularly tested against adversarial evasion attacks and to report the results of such testing to the Financial Intelligence Unit.[740]

Third, SEBI should develop a comprehensive regulatory framework for AI-driven algorithmic trading that goes beyond the existing provisions of its algorithmic trading circulars to specifically address self-optimising and self-learning trading algorithms, real-time market manipulation detection, and the explainability requirements for algorithms whose trading decisions may be the subject of enforcement proceedings.[825]

Fourth, the Information Technology Act 2000, or its successor legislation, should be amended to criminalise the creation and deployment of deepfakes for fraudulent purposes, including corporate identity fraud, securities manipulation and fraudulent payment authorisation. Hartzog's concept of privacy by design should inform the development of technical standards for the authentication of digital media in corporate and financial contexts.[2934]

Fifth, India should invest substantially in the AI capacity of its enforcement agencies the Central Bureau of Investigation, the Enforcement Directorate, the Serious Fraud Investigation Office and the Income Tax Department providing them with access to state-of-the-art AI forensic tools and the expertise necessary to deploy them effectively in the investigation and prosecution of complex financial offences.[3337]

Sixth, India should pursue active engagement in the development of international legal standards for AI-facilitated financial crime through the Financial Action Task Force, INTERPOL, the G20 and bilateral treaty arrangements, recognising that many of the most significant AI-enabled white-collar offences are transnational in character and require coordinated international responses.[386]

VII. CONCLUSION

White collar crime and artificial intelligence have become inextricably entangled, and the consequences of this entanglement for economic security, market integrity and public trust are profound. The great Satyam scandal of 2008 — which exposed the vulnerability of India's corporate governance architecture to sophisticated accounting fraud demonstrated what white collar crime at scale could do to investor confidence and economic stability in the pre-AI era.[36] The AI era threatens to produce harms of a qualitatively different order: faster, more scalable, more difficult to detect and attribute, and more deeply embedded in the algorithmic infrastructure of modern economic life.[11]

The regulatory and legislative response must be equal to this challenge. Piecemeal amendments to existing statutes, supplemented by non-binding circulars and guidelines, are no longer adequate. India needs a coherent, forward-looking legal architecture one that criminalises AI-facilitated financial misconduct with clarity, equips enforcement agencies with the tools and resources necessary to investigate it effectively, and engages constructively with the emerging body of international law and regulatory practice in this domain.[3040]

The challenge is urgent, but it is not insuperable. Law has always adapted to technological change from the telegraph to the telephone to the internet and it will adapt again. The question is whether the adaptation will be rapid enough to keep pace with the unprecedented velocity of change that AI represents, and whether India will play a proactive rather than a reactive role in shaping the global legal response to this defining challenge of the twenty-first century.[39]

FOOTNOTES

[1.] Edwin H. Sutherland, White Collar Crime (New York: Dryden Press, 1949), p. 9.
[2.] Stuart P. Green, Lying, Cheating, and Stealing: A Moral Theory of White-Collar Crime (Oxford: Oxford University Press, 2006), pp. 14–17.
[3.] Europol, Internet Organised Crime Threat Assessment (IOCTA) 2023 (The Hague: Europol, 2023), p. 12.
[4.] Federal Bureau of Investigation, Internet Crime Report 2023 (Washington D.C.: FBI, 2024), p. 4.
[5.] PricewaterhouseCoopers, Global Economic Crime and Fraud Survey 2022 (London: PwC, 2022), p. 7.
[6.] Anil Kalhan et al., 'Colonial Continuities: Human Rights, Terrorism, and Security Laws in India,' Columbia Journal of Asian Law, Vol. 20, No. 1 (2006), pp. 93–234.
[7.] Prevention of Money Laundering Act, 2002 (Act No. 15 of 2003), Government of India, Ministry of Finance.
[8.] Securities and Exchange Board of India, Annual Report 2022–23 (Mumbai: SEBI, 2023), p. 45.
[9.] N. Rattan, Corporate Frauds and White Collar Crimes in India (Delhi: Universal Law Publishing, 2020), pp. 88–92.
[10.] Andrew Burt & Dan Geer, 'The Liability Problem for Future Cybersecurity,' Lawfare Blog, September 2017.
[11.] Varun Bali, 'AI-Driven Financial Crimes: Emerging Typologies and Regulatory Response,' Journal of Financial Crime, Vol. 30, No. 2 (2023), pp. 415–430.
[12.] Financial Stability Board, Artificial Intelligence and Machine Learning in Financial Services (Basel: FSB, 2017),
p. 22.
[13.] Nicola Ryder, Financial Crime in the 21st Century: Law and Policy (Cheltenham: Edward Elgar, 2011), pp. 134–
138.
[14.] Europol, Facing Reality? Law Enforcement and the Challenge of Deepfakes (The Hague: Europol, 2022), p. 5.
[15.] Hao Li et al., 'Advancing High Fidelity Identity Swapping for Forgery Detection,' Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition (2020), pp. 5073–5082.
[16.] Federal Trade Commission, Consumer Sentinel Network Data Book 2023 (Washington D.C.: FTC, 2024), p. 9.
[17.] Shoshana Zuboff, The Age of Surveillance Capitalism (New York: PublicAffairs, 2019), pp. 233–240.
[18.] Shlomit Yanisky-Ravid & Sean Hallisey, 'Equality and Privacy by Design: A New Model of Artificial Intelligence Data Transparency via Auditing, Certification and Safe Harbor Regimes,' Fordham Urban Law Journal, Vol. 46, No. 2 (2019), pp. 428–486.
[19.] Deidre Mulligan & Kenneth Bamberger, 'Saving Governance-By-Design,' California Law Review, Vol. 106, No. 3 (2018), pp. 697–784.
[20.] Abhishek Dubey, 'Algorithmic Collusion and Competition Law: An Indian Perspective,' Indian Journal of Law and Technology, Vol. 17 (2021), pp. 55–78.
[21.] Competition Commission of India, Market Study on E-Commerce in India (New Delhi: CCI, 2020), pp. 62–67.
[22.] KPMG, The War Against Money Laundering: How AI is Transforming Financial Crime Compliance (London: KPMG, 2023), p. 11.
[23.] Mihail Popescu, 'Machine Learning Models for Financial Crime Detection: A Survey,' Expert Systems with Applications, Vol. 196 (2022), pp. 116–125.
[24.] Securities and Exchange Commission, 'SEC Charges Algorithm-Based Trading Firm for Market Manipulation,' Press Release No. 2023-91 (Washington D.C.: SEC, 2023).
[25.] Niamh Moloney, EC Securities Regulation, 3rd ed. (Oxford: Oxford University Press, 2014), pp. 774–780.
[26.] Ministry of Electronics and Information Technology, National Strategy for Artificial Intelligence (New Delhi: NITI Aayog, 2018), pp. 35–38.
[27.] Reserve Bank of India, Report of the Working Group on Digital Lending including Lending through Online Platforms and Mobile Apps (Mumbai: RBI, 2021), pp. 29–33.
[28.] European Parliament and Council, Regulation (EU) 2024/1689 on Artificial Intelligence (AI Act) (Brussels: Official Journal of the European Union, 2024).
[29.] Woodrow Hartzog, Privacy's Blueprint: The Battle to Control the Design of New Technologies (Cambridge: Harvard University Press, 2018), pp. 201–215.
[30.] Vivek Sehgal, 'Regulating AI in India: A Sectoral Approach,' National Law School of India Review, Vol. 34, No. 1 (2022), pp. 88–110.
[31.] Pavan Duggal, Cyber Law: The Indian Perspective, 3rd ed. (New Delhi: Saakshar Law Publications, 2020), pp. 177–185.
[32.] Srikrishna Committee Report, A Free and Fair Digital Economy: Protecting Privacy, Empowering Indians (New Delhi: Ministry of Electronics and Information Technology, 2018), p. 80.
[33.] Central Bureau of Investigation, Annual Report 2022–23 (New Delhi: CBI, 2023), pp. 19–23.
[34.] Yoti & Centre for Emerging Technology and Security, Deepfakes and Cheap Fakes: The Manipulation of Audio and Visual Evidence (London: Alan Turing Institute, 2023), p. 17.
[35.] Tim Wu, The Curse of Bigness: Antitrust in the New Gilded Age (New York: Columbia Global Reports, 2018), pp. 112–118.

[36.] Nidhi Singh, 'Satyam Scandal and Corporate Governance Failures in India,' Corporate Law Journal, Vol. 8 (2009), pp. 44–60.
[37.] Serious Fraud Investigation Office, Annual Report 2022–23 (New Delhi: SFIO, 2023), pp. 8–14.
[38.] INTERPOL, Financial Crimes Unit Report 2023 (Lyon: INTERPOL, 2023), p. 22.
[39.] Viktor Mayer-Schonberger & Kenneth Cukier, Big Data: A Revolution That Will Transform How We Live, Work and Think (London: John Murray, 2013), pp. 155–162.
[40.] Kiran Gupta, 'Liability Frameworks for AI-Generated Financial Misconduct: Lessons for India,' NALSAR Law Review, Vol. 15 (2023), pp. 110–134.

REFERENCES

A. Books and Monographs

Burt, Andrew & Geer, Dan, 'The Liability Problem for Future Cybersecurity', Lawfare Blog, September 2017.

Duggal, Pavan, Cyber Law: The Indian Perspective, 3rd ed. (New Delhi: Saakshar Law Publications, 2020).

Green, Stuart P., Lying, Cheating, and Stealing: A Moral Theory of White-Collar Crime (Oxford: Oxford University Press, 2006).

Hartzog, Woodrow, Privacy's Blueprint: The Battle to Control the Design of New Technologies (Cambridge: Harvard University Press, 2018).

Mayer-Schonberger, Viktor & Cukier, Kenneth, Big Data: A Revolution That Will Transform How We Live, Work and Think (London: John Murray, 2013).

Moloney, Niamh, EC Securities Regulation, 3rd ed. (Oxford: Oxford University Press, 2014).

Rattan, N., Corporate Frauds and White Collar Crimes in India (Delhi: Universal Law Publishing, 2020). Ryder, Nicola, Financial Crime in the 21st Century: Law and Policy (Cheltenham: Edward Elgar, 2011). Sutherland, Edwin H., White Collar Crime (New York: Dryden Press, 1949).

Wu, Tim, The Curse of Bigness: Antitrust in the New Gilded Age (New York: Columbia Global Reports, 2018).

Zuboff, Shoshana, The Age of Surveillance Capitalism (New York: PublicAffairs, 2019).

B. Journal Articles

Bali, Varun, 'AI-Driven Financial Crimes: Emerging Typologies and Regulatory Response', Journal of Financial Crime, Vol. 30, No. 2 (2023), pp. 415–430.

Dubey, Abhishek, 'Algorithmic Collusion and Competition Law: An Indian Perspective', Indian Journal of Law and Technology, Vol. 17 (2021), pp. 55–78.

Gupta, Kiran, 'Liability Frameworks for AI-Generated Financial Misconduct: Lessons for India', NALSAR Law Review, Vol. 15 (2023), pp. 110–134.

Kalhan, Anil et al., 'Colonial Continuities: Human Rights, Terrorism, and Security Laws in India', Columbia Journal of Asian Law, Vol. 20, No. 1 (2006), pp. 93–234.

Li, Hao et al., 'Advancing High Fidelity Identity Swapping for Forgery Detection', Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition (2020), pp. 5073–5082.

Mulligan, Deidre & Bamberger, Kenneth, 'Saving Governance-By-Design', California Law Review, Vol.

106, No. 3 (2018), pp. 697–784.

Popescu, Mihail, 'Machine Learning Models for Financial Crime Detection: A Survey', Expert Systems with Applications, Vol. 196 (2022), pp. 116–125.

Sehgal, Vivek, 'Regulating AI in India: A Sectoral Approach', National Law School of India Review, Vol.

34, No. 1 (2022), pp. 88–110.

Singh, Nidhi, 'Satyam Scandal and Corporate Governance Failures in India', Corporate Law Journal, Vol.

8 (2009), pp. 44–60.

Yanisky-Ravid, Shlomit & Hallisey, Sean, 'Equality and Privacy by Design', Fordham Urban Law Journal, Vol. 46, No. 2 (2019), pp. 428–486.

C. Reports, Statutes and Official Documents

Central Bureau of Investigation, Annual Report 2022–23 (New Delhi: CBI, 2023).

Competition Commission of India, Market Study on E-Commerce in India (New Delhi: CCI, 2020). European Parliament and Council, Regulation (EU) 2024/1689 on Artificial Intelligence (AI Act)

(Brussels: Official Journal of the European Union, 2024).

Europol, Facing Reality? Law Enforcement and the Challenge of Deepfakes (The Hague: Europol, 2022). Europol, Internet Organised Crime Threat Assessment (IOCTA) 2023 (The Hague: Europol, 2023).

Federal Bureau of Investigation, Internet Crime Report 2023 (Washington D.C.: FBI, 2024).

Federal Trade Commission, Consumer Sentinel Network Data Book 2023 (Washington D.C.: FTC, 2024).

Financial Stability Board, Artificial Intelligence and Machine Learning in Financial Services (Basel: FSB, 2017).

INTERPOL, Financial Crimes Unit Report 2023 (Lyon: INTERPOL, 2023).

KPMG, The War Against Money Laundering: How AI is Transforming Financial Crime Compliance (London: KPMG, 2023).

Ministry of Electronics and Information Technology, National Strategy for Artificial Intelligence (New Delhi: NITI Aayog, 2018).

PricewaterhouseCoopers, Global Economic Crime and Fraud Survey 2022 (London: PwC, 2022). Prevention of Money Laundering Act 2002 (Act No. 15 of 2003), Government of India, Ministry of

Finance.

Reserve Bank of India, Report of the Working Group on Digital Lending (Mumbai: RBI, 2021).

Securities and Exchange Board of India, Annual Report 2022–23 (Mumbai: SEBI, 2023).

Serious Fraud Investigation Office, Annual Report 2022–23 (New Delhi: SFIO, 2023).

Srikrishna Committee Report, A Free and Fair Digital Economy (New Delhi: MEITY, 2018).

Yoti & Centre for Emerging Technology and Security, Deepfakes and Cheap Fakes (London: Alan Turing Institute, 2023).

United States Securities and Exchange Commission, SEC Charges Algorithm-Based Trading Firm for Market Manipulation, Press Release No. 2023-91 (Washington D.C.: SEC, 2023).