International Journal of Interdisciplinary Cultural Studies
ISSN: 2327-008X (Print), ISSN: 2327-2554 (Online)
Volume 20, Issue 2, 2025
https://cgscopus.com/index.php/journals
Scopus

GOVERNING INVISIBLE ACTORS - A CRITICAL EVALUATION OF INDIA'S REGULATORY VACUUM IN AI-INDUCED CRIMES

Priya Bairagi, Research Scholar, Jamnalal Bajaj School of Legal Studies, Banasthali Vidyapith

Dr. Asha Rawat, Assistant Professor, Faculty of Law, Jamnalal Bajaj School of Legal Studies, Banasthali Vidyapith

ABSTRACT

Artificial Intelligence (AI) has transformed the nature of crime globally, enabling new forms of digital impersonation, algorithmic manipulation, predictive profiling, and autonomous cyber-attacks. In India, the adoption of AI by both legitimate sectors and malicious actors has accelerated rapidly, yet the regulatory landscape remains fragmented, technologically outdated, and normatively incomplete. This paper critically evaluates the emerging phenomenon of AI-induced crimes within the Indian context, with a particular focus on the deepening regulatory vacuum. Drawing upon contemporary scholarship, comparative regulatory models, and evolving forms of cyber-criminal behavior, the analysis demonstrates that Indian law lacks clear statutory provisions, institutional capacities, and doctrinal clarity for addressing harms created by non-human, autonomous, or semi-autonomous digital agents. The paper argues that India requires a paradigm shift, from a human-centric responsibility model to a techno-normative framework capable of attributing liability, regulating AI development, and preventing abuse. Through a doctrinal and socio-legal examination, this study outlines conceptual challenges, identifies gaps in the Information Technology Act, 2000, and highlights the urgency of designing a future-ready governance architecture for AI-induced criminality.

Keywords - Artificial Intelligence, AI-Induced Crimes, Cyber Law, Regulatory Vacuum, India, Algorithmic Accountability, IT Act, Digital Impersonation, Liability, Autonomous Systems.

BACKGROUND

The mainstreaming of AI across financial systems, governance platforms, telecommunications, and social media ecosystems has radically altered the nature of criminality. Crimes no longer require human presence, intent, or even direct execution; instead, algorithmic entities and machine-learning systems are increasingly capable of generating harm autonomously. Scholars have described these phenomena as "synthetic criminality" or "autonomous harmful conduct," wherein the digital environment becomes populated by actors whose behavior cannot be predicted or regulated through traditional legal doctrines (Calo, 2015; Goldenfein & Leiter, 2022). In India, the rapid digitization of public services, expansion of biometric infrastructures, and unregulated growth of AI start-ups have created an ecosystem particularly vulnerable to AI-enabled harms.

While nations such as the European Union and the United States have begun constructing AI-specific regulatory frameworks, India continues to rely on the Information Technology Act, 2000, which was enacted long before contemporary AI architectures emerged. As a result, crimes involving deepfakes, AI-generated impersonation, autonomous malware, algorithmic financial fraud, and predictive manipulation remain legally ambiguous. The absence of statutory definitions, forensic tools, reporting protocols, and liability standards creates a vacuum that allows malicious actors to operate invisibly and with near impunity (NITI Aayog, 2021).

UNDERSTANDING THE EXPANDING SPECTRUM OF AI-INDUCED CRIMINALITY IN THE INDIAN DIGITAL ECOSYSTEM

AI-induced crimes refer to offences in which AI either facilitates, enhances, or autonomously performs harmful activities. The definitional complexity arises because AI systems do not behave like traditional tools; they learn, adapt, and sometimes act in ways unforeseen even by their developers (Rahwan et al., 2019). In India, the expansion of digital infrastructure has led to at least four major categories of AI-related criminal conduct.

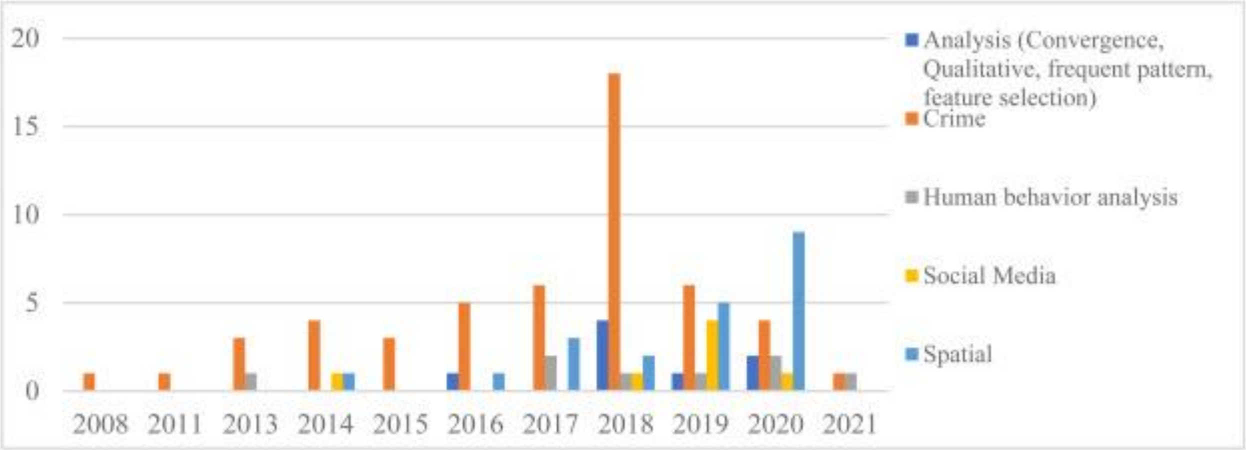
The integration of biometric systems such as Aadhaar into welfare schemes and financial transactions has increased India's vulnerability to AI-based identity manipulation. Deepfake technology allows criminals to create hyper-realistic videos or audio clips impersonating political figures, judges, corporate officers, or family members. Studies indicate that India ranks among the top countries exposed to deepfake-enabled social engineering fraud

(Kaspersky, 2023). AI-driven impersonation has already been used to bypass e-KYC checks, enabling unauthorized withdrawals, fake loan applications, and fraudulent digital signatures (Sharma & Bedi, 2022). The Indian Evidence Act does not explicitly regulate deepfake authentication, creating uncertainty regarding admissibility and reliability. Similarly, the IT Act lacks provisions addressing synthetic media or algorithmic falsification. This legal gap allows malicious actors to manipulate public opinion, distort political narratives, perpetrate financial fraud, and compromise personal dignity, without a clear pathway for prosecution (Yadav & Sharma, 2025).

Traditional cybercrime requires a human operator; however, AI-generated cyber-attacks can self-propagate, evade detection, and autonomously exploit vulnerabilities. Research indicates that machine-learning algorithms can be trained to design polymorphic malware that mutates faster than existing security systems can respond (Brundage et al., 2018). For a country like India, where over 800 million people are internet-users but cybersecurity literacy remains low, the consequences of autonomous malware can be catastrophic. Government reports acknowledge repeated attacks on Indian banking institutions, critical infrastructure, and public databases, some of which involve automated systems capable of overwhelming networks without manual intervention (CERT-In, 2023). Yet Indian cyber law does not distinguish between malware created by a human and malware developed or evolved by an AI system. This doctrinal silence complicates attribution, as culpability often hinges on concepts like intention or knowledge, elements that do not map neatly onto AI systems. AI also enables new forms of financial and market-based manipulation. High-frequency trading bots, recommendation algorithms, and fraud-detection systems can be repurposed to engage in market distortions or consumer deception. Algorithmic collusion, where pricing algorithms unintentionally coordinate with one another, has already raised antitrust concerns globally (Ezrachi & Stucke, 2016).

In India, AI-driven financial scams have increased significantly, with fraudsters using predictive models to identify potential victims and generate personalized phishing messages at scale (Rao, 2022). Criminals use reinforcement-learning systems to optimize fraud strategies in real-time, making traditional enforcement reactive and often ineffective. The Securities and Exchange Board of India (SEBI) currently lacks dedicated regulatory clauses for algorithmic crimes, while the Reserve Bank of India (RBI) has issued only advisory guidelines for digital fraud risks. No statute directly addresses liability for AI-driven market manipulation, leaving victims without clear remedies. AI-generated text, images, and datasets have been exploited for misinformation campaigns, extremist propaganda, and dark-web marketplaces. Language models capable of generating realistic human-like conversation enable criminals to automate grooming, radicalization, and recruitment (Weidinger et al., 2021). These tools significantly reduce the labor required for large-scale influence operations.

Given India's socio-political diversity and susceptibility to communal tensions, such automated disinformation poses severe risks. However, the legal framework remains limited to provisions on electronic defamation and incitement, none of which account for algorithmic propagation, synthetic speech, or automated amplification. Enforcement agencies, already overburdened, lack the technological capacity to trace AI-generated content to its origin (Shukla, 2025).



Source – https://www.sciencedirect.com/science/article/pii/S2590291122000961

THE CORE PROBLEMS IN ASSIGNING LEGAL RESPONSIBILITY AND CRIMINAL LIABILITY TO AI SYSTEMS IN INDIA

One of the most fundamental challenges in regulating AI-induced crimes is the difficulty of mapping traditional legal constructs, such as mens rea, actus reus, causation, and foreseeability, onto non-human agents. Indian law presumes a human offender who intentionally or recklessly engages in unlawful conduct. AI systems, however, may produce harmful outcomes without direct human commands. Scholars have described this problem as a "liability gap," wherein neither the developer nor the user can be clearly held accountable for autonomous harmful behavior (Pagallo, 2013; Abbott & Sarch, 2019). For India, this gap is magnified by institutional limitations, outdated cyber-forensics infrastructure, and the absence of doctrinal guidance in criminal jurisprudence.

Mens rea, or the mental element of crime, requires intention, knowledge, recklessness, or negligence. AI systems do not possess mental states; they operate through probabilistic models, pattern recognition, and optimization. Indian courts have no precedent for applying intention-based standards to machines. Thus, when an autonomous system commits harm, determining whether the developer, deployer, or user "intended" or "knew" the consequences becomes legally ambiguous. The IT Act criminalizes unauthorized access, identity theft, cheating through computer resources, and publishing sexually explicit content. However, the Act was drafted at a time when AI was not envisioned as an autonomous actor. As scholars have noted, applying outdated statutory language to modern AI systems results in interpretive distortions and inconsistent enforcement (Katyal, 2019). India lacks legal doctrines recognizing shared liability, distributed decision-making, or algorithmic agency.

DOCTRINAL AND STRUCTURAL WEAKNESSES IN INDIA'S CYBER-LEGAL ARCHITECTURE ENABLING A REGULATORY VACUUM

India's inadequacy in addressing AI-induced crimes stems not merely from the absence of explicit statutory provisions but from deeper doctrinal weaknesses within its cyber-legal architecture. The Information Technology Act, 2000 was drafted in an era when cyberspace was conceived as a domain of static websites, rudimentary hacking, and basic electronic signatures. With the emergence of generative AI, deep learning, reinforcement-learning agents, and autonomous malware, the Act's vocabulary and scope have become insufficient. Scholars have repeatedly emphasized that the mismatch between technological realities and legislative frameworks creates a legal void in which harmful AI operations can occur unchecked (Chander, 2021; Bhandari, 2023). As India's digital infrastructure expands, the structural gaps in the IT Act and related regulations pose critical obstacles to effective governance.

A foundational limitation lies in the Act's anthropocentric assumption that criminal behavior originates from human actors who manipulate computer resources. Sections 43, 66, and 66C, for example, require establishing that a person "accessed," "caused," or "dishonestly used" computer resources. AI systems, however, can independently initiate harmful processes without direct human commands. This divergence makes it difficult for enforcement agencies to frame charges, leading to procedural delays and low conviction rates. Furthermore, the Act does not provide standards for attributing responsibility in cases involving complex AI supply chains composed of developers, data providers, deployers, and users. Without a framework for distributed accountability, liability becomes diffused to the point of legal irrelevance (Singh, 2025).

Compounding this issue is the insufficient integration of AI governance mechanisms across sectoral regulators. Agencies such as the Reserve Bank of India, SEBI, and the Telecom Regulatory Authority of India issue advisory guidelines to manage AI-related risks, but these advisories lack statutory enforceability. As a result, corporations and financial institutions often adopt AI tools without undergoing regulatory audits or risk evaluations. In high-stakes sectors such as fintech, insurance, and telecommunications, unregulated AI deployment heightens the possibility of both intentional misuse and accidental harm (Chakraborty, 2022). The fragmented architecture prevents the emergence of a unified national approach to AI safety, ethics, and criminal liability.

CHALLENGES IN ENFORCEMENT - INSTITUTIONAL CAPACITY, FORENSICS, AND POLICING AI-GENERATED CRIMES

Even if statutory reforms were introduced, India faces significant enforcement challenges due to the limited capacity of policing and forensic institutions to investigate AI-induced crimes. The complexity of machine-learning systems, the opacity of neural networks, and the cross-border nature of digital operations demand advanced investigative infrastructures. Yet India's current capabilities remain heavily dependent on manual investigation techniques and outdated forensic tools (Mishra & Thaplu, 2025).

The problem begins with the lack of specialized AI-forensics units within law enforcement agencies. Traditional cyber-forensics focuses on metadata extraction, log analysis, and device imaging. These methods are inadequate for evaluating autonomous system behavior, analyzing adversarial attacks, or detecting deepfake forgeries. Deepfake-detection algorithms deployed globally often rely on micro-expression analysis and GAN-detection frameworks, but Indian police forces rarely have access to such technologies (Agarwal et al., 2020). As a result, AI-generated content spreads rapidly, while investigative bodies struggle to authenticate or trace its origin.

Institutional challenges extend to judicial capacity as well. Indian courts have not developed consistent jurisprudence concerning AI liability. Judges often rely on expert testimony that may itself be inconclusive due to the opacity of machine-learning models. As scholars note, the "black-box" problem severely compromises prosecutorial efforts because it becomes difficult to demonstrate causation, foreseeability, or negligence when the internal logic of the AI system cannot be explained (Burrell, 2016). Without legal recognition of explainability standards or mandatory algorithmic transparency, courts are left with evidentiary gaps that undermine enforcement.

Policing AI crimes is further complicated by jurisdictional ambiguity. AI-induced cyber operations often originate from servers outside India, routed through anonymized networks or cloud infrastructures. India's Mutual Legal Assistance Treaty (MLAT) processes remain slow and bureaucratic, hindering timely access to foreign evidence (Singh, 2023). Malicious actors exploit these delays by continuously migrating their digital infrastructures. Even when investigators trace harmful content, the server logs may already be deleted, encrypted, or stored in jurisdictions with weak cooperation agreements.

The challenges are compounded by the fact that many AI-induced crimes involve rapid, large-scale harm. Deepfake pornography targeting women can circulate across millions of devices within hours, causing irreparable reputational damage. Autonomous financial scams powered by AI can generate thousands of fraudulent transactions before banks detect anomalies. These realities require high-speed forensic intervention, but India currently lacks the technological agility and inter-agency coordination needed for such responses (Zucca, & Fiorinelli, 2025).

COMPARATIVE INSIGHTS FROM GLOBAL APPROACHES TO REGULATING AI-ENABLED CRIMINAL BEHAVIOUR

To address India's regulatory vacuum, a comparative study of global AI governance frameworks offers valuable insights. While no jurisdiction has fully resolved the problem of criminal liability for autonomous systems, countries such as the European Union, the United States, and the United Kingdom have taken significant steps toward regulating AI-induced harms through risk classification, algorithmic transparency, and developer accountability.

The EU Artificial Intelligence Act (2024) represents the world's most comprehensive attempt to regulate AI. It classifies AI systems into categories based on risk, unacceptable, high-risk, limited, and minimal, thereby imposing varying levels of compliance obligations. Importantly, the Act mandates robustness, cybersecurity safeguards, human oversight, and detailed documentation for high-risk systems. Although the Act is primarily focused on civil and regulatory compliance, its provisions implicitly support criminal enforcement by creating clear audit trails and accountability structures (Veale & Zuiderveen Borgesius, 2021).

For India, the EU model demonstrates that managing AI-induced crimes requires embedding safety and transparency requirements at the design stage, rather than relying solely on post-hoc criminal liability. Mandatory risk assessment and algorithmic documentation could significantly assist prosecutorial efforts by clarifying who controlled the system, what parameters influenced its decisions, and whether the harm was foreseeable. The United States does not have a federal AI law, but several agencies have issued guidelines addressing AI misuse. The Federal Trade Commission (FTC) enforces AI-related deception, discriminatory algorithms, and data misuse through existing consumer protection statutes. Meanwhile, the National Institute of Standards and Technology (NIST) has developed the AI Risk Management Framework (2023), which sets standards for transparency, safety, and monitoring. Scholars argue that the U.S. is increasingly moving toward corporate liability for harmful AI deployments, particularly when developers fail to implement adequate safeguards (Crootof & Ard, 2022).

India can draw from this approach by establishing statutory obligations for developers and deployers, including mandatory auditing, documentation, and risk mitigation. An expanded liability regime could ensure that corporate actors cannot evade responsibility when their AI systems facilitate fraud, misinformation, or privacy violations. The UK has adopted a decentralized but principles-based model, outlined in its AI White Paper. Instead of a single AI statute, the model empowers existing regulators, such as financial, healthcare, and data-protection agencies, to interpret common AI governance principles including safety, fairness, accountability, contestability, and redressability (Oswald, 2023). Although flexible, this approach has been criticized for lacking statutory force, which may weaken enforcement. However, the UK model demonstrates the value of inter-regulatory coordination. A national AI coordination office ensures harmonization across sectors. India, which currently suffers from fragmented regulatory action, may benefit from establishing a similar coordination mechanism under the Ministry of Electronics and Information Technology.

NEED FOR A NEW LEGAL PARADIGM: WHY INDIA MUST REDESIGN ITS CRIMINAL JUSTICE FRAMEWORK FOR AI HARMS

The preceding sections demonstrate that India cannot rely on incremental amendments to the IT Act or piecemeal advisories. A systemic transformation is necessary because AI-induced harms challenge the fundamental assumptions of Indian criminal law. The actus reus–mens rea model, the anthropocentric liability framework, and the judicial evidence standards were designed for human behaviour, not autonomous agents. AI systems often operate according to emergent behavior, probabilistic decision-making, and opaque logic, making it difficult to attribute intention or foreseeability. Moreover, as machine-learning systems evolve, the line between tool and actor blurs. Scholars argue that modern AI challenges the moral and legal boundaries that distinguish instruments from autonomous agents (Gunkel, 2017). In India, where doctrinal evolution in criminal law is conservative and incremental, adapting to these changes requires both conceptual and institutional innovation.

A redesigned framework must therefore include statutory recognition of algorithmic agency, principles of shared liability, mandatory AI audits, digital forensic modernization, and dedicated AI investigation units. Without these reforms, India risks becoming a jurisdiction where AI-induced crimes flourish unchecked, with profound implications for privacy, financial security, national security, and democratic integrity (Putra, 2025).

TOWARDS A COMPREHENSIVE REGULATORY ARCHITECTURE

India’s response to AI-induced crimes must move beyond incremental legislative adjustments and embrace a holistic, multi-layered framework that integrates doctrinal reform, institutional restructuring, technological modernization, and inter-agency coordination. Emerging scholarship on algorithmic governance, platform regulation, and cyber-criminal liability emphasizes that effective AI regulation requires combining ex-ante preventive mechanisms with ex-post enforcement tools (Calo, 2021; Citron, 2024). For India, this implies designing a legal architecture that anticipates harm rather than reacting to it after the fact.

The first pillar of such a framework is the introduction of a dedicated AI (Regulation and Accountability) Act, which should establish legal definitions, allocate liability, and set standards for safe AI development and deployment. The Act must clearly define concepts such as autonomous systems, high-risk AI, algorithmic manipulation, biometric content synthesis, and automated decision-making. Moreover, the legislation must identify responsible actors in the AI lifecycle, developers, trainers, data suppliers, deployers, platform intermediaries, and end users, and delineate their obligations. A statutory architecture that internalizes accountability at each stage would prevent the diffusion of responsibility that currently characterizes AI-related harm.

The second pillar requires establishing criminal liability frameworks tailored to AI operations. Traditional mens rea doctrines, such as intention and knowledge, do not map neatly onto autonomous algorithmic behavior. India should therefore adopt hybrid liability models that integrate principles of negligence, strict liability, and vicarious responsibility. In situations where developers fail to implement adequate safeguards, provide transparency, or mitigate foreseeable risks, strict liability provisions may be appropriate, particularly in high-risk sectors such as finance, biometric surveillance, cybersecurity, and critical infrastructure.

Additionally, India must create statutory offences that explicitly address AI-induced harms, such as malicious deepfake creation, automated phishing campaigns using generative models, autonomous malware deployment, and AI-powered identity fraud. Explicit criminalization would allow law enforcement agencies to bypass interpretive uncertainties associated with stretching the definitions under the IT Act, thereby enabling more efficient prosecution.

CONCLUSION

India presently finds itself at a pivotal crossroads in its technological trajectory, where the rapid proliferation of artificial intelligence demands a corresponding evolution of legal doctrine and institutional machinery. Although the revolutionary potential of AI, particularly systems capable of autonomous decision-making, is now firmly established, the country's normative and regulatory architecture has not advanced at a pace commensurate with these developments. The disjunction between technological capability and legal preparedness has created a structural void, one that is not attributable merely to the absence of explicit statutory provisions, but also to entrenched doctrinal rigidities, administrative inertia, and the limited technical orientation of the criminal justice apparatus. As demonstrated throughout this paper, India's inability to articulate a coherent framework for regulating self-learning, harm-causing systems reflects deeper systemic constraints that transcend conventional legislative drafting.

The prevailing cyber-legal regime, grounded primarily in the Information Technology Act of 2000 and its subsidiary rules, is manifestly ill-equipped to adjudicate and regulate harms emerging from advanced AI operations. Crafted at a time when algorithms lacked autonomy and were incapable of iterative self-modification, this framework remains heavily anthropocentric and presumes a direct causal link between human agency and technological misuse. Such a construct is fundamentally incompatible with the operational realities of contemporary AI, which can act independently of the programmer’s intention and evolve beyond its initial design parameters. The absence of provisions recognizing machine autonomy, coupled with antiquated enforcement mechanisms that rely on traditional evidentiary and investigative processes, creates vast regulatory blind spots. These deficiencies are compounded by the limited forensic capacity to trace algorithmic decision-making, sluggish international cooperation in cyber investigations, and a fractured regulatory environment populated by overlapping, and at times conflicting, institutional mandates. As a result, malicious AI-driven activities continue to exploit the systemic disconnect between dynamic technological processes and static statutory frameworks, enabling actors to evade accountability with relative ease.

A comparative examination of foreign jurisdictions underscores the urgency of recalibrating India’s regulatory posture. The European Union’s risk-tiered regulatory model, the United States’ emerging sectoral governance mechanisms, and the United Kingdom’s emphasis on accountability-by-design collectively demonstrate a global shift toward embedding safeguards at the developmental and operational stages of AI systems. These jurisdictions have begun integrating ex ante obligations, such as algorithmic transparency, safety testing, continuous monitoring, and documentation requirements, into their legal regimes, reflecting an appreciation that traditional post-incident liability models are inadequate for technologies capable of causing instantaneous, widespread harm. While these frameworks are not devoid of limitations, they provide instructive evidence that regulatory foresight, rather than retrospective criminal attribution, is essential for mitigating the dangers posed by autonomous systems.

REFERENCES

- Agarwal, S., Farid, H., Gu, Y., He, M., Nagano, K., & Li, H. (2020). *Detecting deep-fake videos from appearance and behavior*. IEEE Journal of Selected Topics in Signal Processing, 14(5), 1039–1052. https://doi.org/10.1109/JSTSP.2020.3007009
- Bhandari, V. (2023). *Artificial intelligence and the future of cyber law in India*. NUJS Law Review, 16(2), 221–245.
- Burrell, J. (2016). How the machine 'thinks': Understanding opacity in machine learning algorithms. *Big Data & Society*, 3(1), 1–12. https://doi.org/10.1177/2053951715622512
- Calo, R. (2021). Artificial intelligence policy: A primer and roadmap. *UC Davis Law Review*, 55, 123–169.
- Chakraborty, S. (2022). Autonomous systems and regulatory challenges in India's financial sector. *Journal of Financial Regulation and Compliance*, 30(3), 289–304.
- Chander, A. (2021). The governance of artificial intelligence. *Emory Law Journal*, 70(6), 1231–1276.
- Citron, D. K. (2024). *The fight for privacy: Protecting dignity, identity, and love in the digital age*. Random House.
- Crootof, R., & Ard, B. (2022). Structuring tech company liability. *Harvard Kennedy School Misinformation Review*, 3(1), 1–15. https://doi.org/10.37016/mr-2020-61
- Gunkel, D. (2017). *The machine question: Critical perspectives on AI, robots, and ethics*. MIT Press.
- Mishra, A., & Thaplu, M. (2025). *Artificial Intelligence and Legal Liability in India: Navigating the Challenges of Accountability and Regulation. International Journal for Scientific & Development Research, 10*(5).
- Oswald, M. (2023). A three-pillar approach to AI oversight in the UK. *Computer Law & Security Review*, 49, 105787. https://doi.org/10.1016/j.clsr.2023.105787

- Putra, G. P. (2025). *Artificial Intelligence in Cybersecurity: Legal and Ethical Challenges in Regulating Autonomous Defense Systems*. *Walisongo Law Review (Walrev), 7*(2), 179–194.

- Shukla, M. (2025). *Artificial Intelligence and Cyber Law: Navigating Legal Complexities*. *International Journal of Advance Research, Ideas and Innovations in Technology, 11*(1).

- Singh, P. (2023). Cross-border cybercrime investigations: Challenges for Indian law enforcement. *International Journal of Cyber Criminology*, 17(1), 56–74.

- Singh, P. (2025). *Deepfakes, identity theft, and the dark web: Legal gaps in AI-Generated fraud, an Indian perspective*. *International Journal of Civil Law and Legal Research, 5*(2 B), 103–108.

- Yadav, M., & Sharma, A. (2025). *Indian Privacy Laws and the Need for Reform in Light of Artificial Intelligence*. *International Journal of Social Science Research, 2*(3), 42–55.

- Zucca, M. V., & Fiorinelli, G. (2025). *Regulating AI to Combat Tech-Crimes: Fighting the Misuse of Generative AI for Cyber Attacks and Digital Offences*. *Technology and Regulation, 2025*, 247–262.