Jus Corpus Law Journal

Open Access Law Journal – Copyright © 2026 – ISSN 2582-7820

Editor-in-Chief – Prof. (Dr.) Rhishikesh Dave; Publisher – Ayush Pandey

The Paradox of Artificial Intelligence in Law & Cyber Security: Elucidating Global Uncertainty and Normative Prudence

Prashita Jain[a]

[a]Faculty of Law, University of Delhi, Delhi, India

Received 18 June 2026; *Accepted* 18 July 2026; *Published* 21 July 2026

Every algorithm written to defend a network is also, in the wrong hands, a blueprint for attacking one, and the law, still drafting yesterday's rulebook, has yet to reckon with this. This article examines the legal and policy environment around Artificial Intelligence within the ambit of cybersecurity. India's legal structure is still incompatible with the growing speed of technological influence at present. With the expanding integration of Artificial Intelligence (AI) in law and cybersecurity, through its inclusion in real-time threat detection, automated incident response, and behaviour analytics to defend against sophisticated attacks, it is important to be cognizant of the dynamic between global uncertainty and normative prudence. Through a jurisprudential study of landmark Court verdicts and a comparative international stance, this research aims to unravel the fundamental challenges in counterpoising global scepticism and normative prudence, specifically with reference to the dichotomy of AI being imperative for modern cybersecurity and repositioning defence from a reactive to a proactive stance in law. While this shift enhances resilience against sophisticated cyber threats, it simultaneously generates heightened uncertainty due to the possibility of falling into destructive hands. Therefore, the roots of AI in cybersecurity's arms race are where the guardians of law must use AI faster and more ethically than attackers. The ultimate motive of this paper is to cast light upon the unattended areas of Artificial Intelligence in cybersecurity, where the arms of law are yet to shield its users.

Keywords: *artificial intelligence, normative prudence, cyber threats.*

INTRODUCTION

In the current digital era, cybersecurity is not just a legal framework but also a shield against the uncertainty of Artificial Intelligence. AI is a force redefining the speed, fortification, and complexity of cyber operations on both sides. With new-age technologies and monitoring capabilities, AI has the power to revolutionise cybersecurity and transform legal weaponry. However, this digital revolution comes with an alarming threat: a spike in cybercrimes, fuelled by gaps in regulations and weak enforcement of justice. The case involving Ms Kamya Buch is a significant 2025 Delhi High Court matter, Kamya Buch v JIX5A & Ors.[1], which resulted in a landmark ruling against online defamation, particularly concerning AI-generated deepfakes and morphed explicit content. This case is a milestone for addressing defamation and damage to dignity because of deepfakes. Cyber criminals manipulate this technology to create hoaxes and chaos that undermine and destabilise organisations. In 2024, India saw a wave of ransomware attacks on various financial institutions, including BSNL data breaches exposing over 278GB of sensitive data,[2] Hathway ISP data leak,[3] wherein a hacker exploited the personal data of over 41 million customers, Star Health Insurance leak[4] becoming the victim of a staggering data breach with over 31 million users' data exposed to the dark web, and many more.

AI's presence has grown immensely in core legal functions such as streamlining case references, drafting, analysing evidence, and even assisting in judicial decisions. Yet, what we praise is only one side of the coin. Technological innovation has paradoxically played a major role in the increase in criminal activities. Globally, cybercrime rates have risen. Modern offenders use artificial intelligence to manipulate and scam online users to steal their data. Consequently, the justice system is left with no option but to improvise and strengthen cyber law statutes to combat sophisticated cybercrimes with legal force. The primary actors in this

[1] *Kamya Buch v JIX5A & Ors* (2025) SCC OnLine Del 6428
[2] ''Data Breach in BSNL' Lok Sabha Unstarred Question No 432' (*Sansad*, 2024) <https://sansad.in/getFile/loksabhaquestions/annex/182/AU432_esByvj.pdf?source=pqals> accessed 08 June 2026
[3] 'Security Breach at Indian Internet Service Provider Hathway: Hacker Exposes KYC Data 4 Million Users' *Maktoob Media* (10 January 2024) <https://maktoobmedia.com/public/post?id=82467&slug=security-breach-at-indian-internet-service-isp-provider-hathway-hacker-exposes-kyc-data-4-million-users> accessed 08 June 2026
[4] Mohamed Imranullah S, 'Star Health data leak case: Madras High Court dismisses appeals by cybersecurity services provider' *The Hindu* (12 April 2026) <https://www.thehindu.com/news/national/tamil-nadu/star-health-data-leak-case-madras-high-court-dismisses-appeals-by-cybersecurity-services-provider/article70838282.ece> accessed 09 June 2026

system are cyber offenders, users, police, judges, prosecutors, and the laws governing this ambit. The objective of this study is to underline the need to regulate and enact stringent cyber laws and to highlight the importance of stricter judicial action to counteract the amplification effects of digital propagation.

AI IN CYBERSECURITY (OFFENSIVE VS DEFENSIVE USE)

AI in Cybersecurity refers to the use of machine learning and artificial intelligence to prevent, detect, and handle cyberattacks. This is performed in a speedy, accurate, and comparatively more efficient manner through machine intelligence than through human resources. AI also reinforces the security of organisations and handles data at a mass scale.[5]

Offensive Artificial Intelligence: Offensive AI refers to the recent trend wherein AI is being exploited by cybercriminals to attack internet users in a more sophisticated and large-scale manner. These cyberattacks are carried out for various purposes, ranging from data theft to deepfakes used in phishing attacks. Deepfake technology refers to scams through which hackers develop fake images/sounds via deep learning to impersonate a victim in order to gain access to their digital belongings or blackmail them. In India, creating, sharing, or hosting deepfakes without consent is a punishable cyber offence. Earlier, there were no laws governing such offences, but on October 22, 2025, the Ministry of Electronics and Information Technology (MeitY) took decisive action and announced amendments to the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021.[6] These amendments mark a turning point in India's statutory framework on digital safety.[7]

Defensive Artificial Intelligence: In contrast to offensive artificial intelligence, defensive AI refers to the use of machine learning and artificial intelligence to proactively detect, prevent, and respond to cyber threats and adversarial attacks. This system is designed to counter both manual and AI-generated cyberattacks. It equips organisations with the ability to anticipate and analyse threats, fight attacks, and automate threat responses. Several AI tactics, such as

[5] Jade Hill, 'Understanding Offensive AI vs. Defensive AI in Cybersecurity' (*Abnormal*, 16 December 2024) <https://abnormal.ai/blog/offensive-ai-defensive-ai> accessed 10 June 2026
[6] Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules 2021
[7] *Explanatory Note: Proposed Amendments to the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021 in relation to synthetically generated information* (Ministry of Electronics and Information Technology, 2025)

anomaly detection, behavioural analytics, and automated threat responses, are used to ensure it stays ahead of attackers, even as they continuously evolve their digital weaponry.

LEGAL AND REGULATORY FRAMEWORK IN INDIA

As we witness the rapid growth of the AI sector, the Indian legal structure still lags. Until recently, cyber hackers took advantage of loopholes in the regulatory framework of the Indian legal system, as there was no law governing AI-enabled digital offences caused by artificial intelligence. The primary reason behind this is that traditional cyber laws rely on human intent and direct causation, making it exceptionally difficult to attribute liability to the developers, deployers, or users of AI systems. AI systems have the independent capability to develop sophisticated malware, including self-replicating worms, evolutionary ransomware, and polymorphic code generators, without direct human programming. Existing legal frameworks face unprecedented challenges in attributing responsibility for the resulting harm. India's Information Technology Act, 2000,[8] designed around traditional human-centric cybercrime models, proves inadequate when confronting scenarios in which machines autonomously generate malicious code that causes substantial damage to digital infrastructure and individual users.[9]

The existing laws comprise constitutional provisions, statutes, rules, regulations, and guidelines across domains such as IT, data protection, intellectual property, entertainment and media, digital employment, consumer protection, and criminal law, indicating that many AI-related risks can be addressed under current laws. Yet, as noted by the Press India Bureau, a comprehensive review is needed as soon as possible for the relevant laws to identify regulatory gaps relating to AI systems, including issues of classification and liability across the AI value chain, application of data protection principles to AI development, misuse of generative AI and challenges around content authentication and provenance, use of copyrighted material in AI training, and sector-specific risks in sensitive domains.

While some of these issues are already under deliberation through inter-ministerial consultations, rulemaking, and expert committees, the rapid evolution of AI, including

[8] Information Technology Act 2000

[9] Aditya Mishra and Himanshu Lohia, 'DIGITAL LIABILITY FOR AI-GENERATED MALWARE: CAN CODE BE A LEGAL PERSON?' (2025) 5(5) Indian Journal of Integrated Research in Law <https://ijirl.com/wp-content/uploads/2025/10/DIGITAL-LIABILITY-FOR-AI-GENERATED-MALWARE-CAN-CODE-BE-A-LEGAL-PERSON.pdf> accessed 10 June 2026

increasingly autonomous systems, poses challenges for regulatory frameworks to remain timely, coherent, and future-ready.[10]

Existing accountability and compliance mechanisms are governed under –

Information Technology Act 2000:[11] Serves as a foundational framework for governing AI alongside newer policies like the Digital Personal Data Protection Act, 2023(DPDP Act)[12] and the India AI Governance Guidelines.[13]

Digital Personal Data Protection Act 2023 (DPDP Act):[14] Mandates a 'privacy by design' framework approach, which ensures that organisations integrate security and consent protocols into their AI development and cybersecurity frameworks.

Section 8(3):[15] Requires organisations to ensure personal data used for automated decisions that affect a person is accurate and complete.

Section 8(5):[16] Mandates reasonable security safeguards to prevent data breaches.

Section 10:[17] Empowers the government to classify entities handling high-risk AI as Significant Data Fiduciaries, subjecting them to audits and impact assessments.

Consumer Protection Act (CPA), 2019:[18] Protects users against deceptive dark patterns of AI designs and over-hyped or misleading claims regarding AI capabilities. AI developers and service providers can be held liable for harm caused by defective AI products or biased algorithms.

[10] 'India AI Governance Guidelines' (*Press Information Bureau,* 15 February 2026) <https://www.pib.gov.in/PressReleasePage.aspx?PRID=2228315> accessed 10 June 2026
[11] Information Technology Act 2000
[12] Digital Personal Data Protection Act 2023
[13] Parin Shah, 'India AI Governance Guidelines: Enabling Safe and Trusted AI Innovation (Part 1)' (*LinkedIn*, 04 December 2025) <https://www.linkedin.com/pulse/india-ai-governance-guidelines-enabling-safe-trusted-innovation-shah-mm7pf/> accessed 10 June 2026
[14] Digital Personal Data Protection Act 2023
[15] Digital Personal Data Protection Act 2023, s 8(3)
[16] Digital Personal Data Protection Act 2023, s 8(5)
[17] Digital Personal Data Protection Act 2023, s 10
[18] Consumer Protection Act 2019

India AI Governance Guidelines: Released by the Ministry of Electronics and Information Technology (MeitY), these guidelines are based on seven core 'sutras,' including human-centric design, transparency, fairness, and accountability.

The Supreme Court of India's Artificial Intelligence Committee issued a notice on June 3, 2026, inviting public feedback on its draft 'Regulations for Use of Artificial Intelligence (AI) in Courts, 2026.'[19] This framework asserts the inclusion of the public and that AI tools must remain strictly assistive, reinforcing human primacy and judicial independence by ensuring that machine outputs never supplant human judgment. These regulations propose strict ethical integration, adherence to fairness, transparency, and data privacy.

LANDMARK JUDICIAL TRENDS IN INDIA

India's legal response to AI-enabled cyber harms has been shaped as much by judicial reasoning as by legislation. In the absence of a dedicated AI statute, constitutional courts have increasingly supplied the interpretive standards that govern privacy, dignity, speech, platform responsibility, and state surveillance in digital contexts. A significant marker of this evolving judicial approach is a formal Record of Proceedings (an official court order)[20] issued by the Hon'ble Supreme Court of India**,** which was initiated after receiving a complaint from a senior citizen couple who were defrauded of their life savings through a 'digital arrest' scam. Since taking notice, numerous other victims have come forward, highlighting a massive, cross-border cybercrime network that heavily targets the public. The Court designated the Central Bureau of Investigation (CBI) as the primary national agency tasked with investigating digital arrest scams across India. Crucially, the court ruled that authorities can freeze these accounts with or without an official FIR being registered, ensuring swift action to preserve victims' stolen funds.

ANI Media Pvt Ltd v OpenAI Inc & Anr: Also, in the matter of ANI Media Pvt Ltd v OpenAI Inc & Anr,[21] which signals the judiciary's early engagement with disputes involving generative AI systems and the legal consequences of their training, outputs, and commercial

[19] 'Seeking views/suggestions of all stakeholders and the general public on draft 'Regulations for Use of Artificial Intelligence (AI) in Courts, 2026' (*European Commission*, 19 June 2026) <https://intellectual-property-helpdesk.ec.europa.eu/news-events/news/seeking-suggestions-all-stakeholders-and-general-public-draft-regulations-use-artificial-2026-06-19_en> accessed 19 June 2026

[20] *In Re: Victims of Digital Arrest Related to Forged Documents* Suo Moto WP (Crl) No 3/2025

[21] *ANI Media Pvt Ltd v OpenAI Inc & Anr* (2024) SCC OnLine Del 8120

deployment. There is no final judgment yet in the landmark copyright lawsuit between Asian News International (ANI) and OpenAI. The Delhi High Court (Justice Amit Bansal) concluded hearings after 32 sittings and officially reserved its verdict. When released, this judgment will serve as India's foundational legal precedent for how artificial intelligence training models interact with national copyright laws.

Pooja Ramesh Singh v Jammu and Kashmir Bank Ltd. & Anr.: Similarly, in the matter of Pooja Ramesh Singh v Jammu and Kashmir Bank Ltd. & Anr.,[22] the Hon'ble Supreme Court of India famously highlighted zero tolerance for unverified AI precedents for presenting, citing or relying on fake or hallucinated AI-generated legal material. The court declared that any judicial decision relying on fake AI- generated material will be treated as "no decision in the eyes of the law" and must be set aside immediately. The Court directed the Bar Council of India to constitute a committee to deliberate on this issue and prescribe guiding principles and disciplinary actions to prevent advocates from submitting fake AI-generated materials.

GLOBAL UNCERTAINTY AND NORMATIVE PRUDENCE REGARDING ARTIFICIAL INTELLIGENCE

Risks of AI to global security include three broad categories of risks: miscalculation, escalation and proliferation. Such risks are interrelated and mutually reinforcing. A lack of understanding of boundaries with AI can lead to overdependence on machines and further escalate to devastating consequences. Recent policy frameworks, including the Secretary-General's 'A New Agenda for Peace', and the first-ever debate on AI at the Security Council in 2023, mentioned the importance of multilateral efforts to mitigate risks and govern the development and use of AI. This report provided a holistic structure for understanding the risks of AI to international peace, global proliferation, and cybersecurity.

Addressing such cybersecurity risks, it can be observed that malicious intent by attackers can derail how an AI system learns and acts. All such risks and executions are closely connected to issues of human–machine interactions and the navigation of governance regarding the liability of offenders.

[22] *Pooja Ramesh Singh v Jammu and Kashmir Bank Ltd & Anr* (2026) INSC 668

AI has the potential to influence International Relations negatively by introducing vulnerabilities, which will impact how States perceive their own strengths relative to others. This can create rifts between the states over competition to achieve AI leadership in defence and the deployment of AI- generated warfare.[23] Concerns have been voiced over recent years about the impact of AI in the coming period, including the possibility of unintentional conflicts, lack of control and inadvertent escalations.[24]

The European Union AI Act[25] addresses aspects of AI-generated harm through risk-based classification and shared liability between the developers and deployers. However, even this legislation falls short of addressing the legal scenarios in which self-learning AI models enter the picture. Such concerns have been raised by legal scholars and experts in the European Parliament Resolution, 2017.[26]

The Artificial Intelligence Basic Act[27] refers to South Korea's framework Act on the development of Artificial Intelligence and Establishment of a Foundation for Trustworthiness. It is one of the world's first comprehensive AI governance laws, balancing industry innovation with strict safety and transparency guardrails for 'High-Impact AI'.

CONCLUSION

Artificial Intelligence is no longer merely a tool in the hands of power; it is woven into the intricacies of daily life. According to the Global AI Diffusion Report published by Microsoft, AI usage increased by 1.5% globally, from 16.3% to 17.8% of the world's working-age population. Across 147 economies, the share of the working-age population using generative AI has steadily increased in recent years.[28] While such figures reflect the growth and evolution of technology, they also highlight the need for urgent regulations and frameworks

[23] Ioana Puscas, *AI and International Security: Understanding the Risks and Paving the Path for Confidence-Building Measures* (UNIDIR 2023)
[24] Michael C Horowitz and Lauren Kahn, 'Leading in Artificial Intelligence through Confidence Building Measures' (2021) 44(4) Washington Quarterly <https://doi.org/10.1080/0163660X.2021.2018794> accessed 12 June 2026
[25] Artificial Intelligence Act 2024
[26] European Parliament Resolution of 16 February 2017 with recommendations to the Commission on Civil Law Rules on Robotics (2015/2103(INL)) [2018] OJ C252/239
[27] Framework Act on the Development of Artificial Intelligence and the Establishment of a Foundation for Trustworthiness 2024
[28] 'Global AI Diffusion: Q1 2026 Trends and Insights' (*Microsoft*) <https://www.microsoft.com/en-us/corporate-responsibility/topics/ai-economy-institute/reports/global-ai-adoption-2026> accessed 12 June 2026

to prevent cyber offences stemming from gaps in governance. In a recent report published by Deloitte, it was revealed that Indian students and employees are 30% more likely to have used generative AI compared to their peers across the Asia-Pacific region. Such figures underscore the need for stricter enforcement of laws and clearer liability frameworks to build a structure suited to the rapidly developing Indian context. India's legal system faces the imperative to evolve beyond traditional, human-centric liability towards more autonomous and sophisticated self-evolving frameworks capable of addressing autonomous artificial agents, while maintaining appropriate accountability and standards to protect victims.

Therefore, the roots of AI in cybersecurity are also where the law must use AI faster and more ethically than attackers. Only then can we say that the Digital India plan has been successfully implemented. Innovation without legal compliance creates unwanted loopholes for attackers and negative consequences without the enforcement of liability.