INDIAN JOURNAL OF LEGAL REVIEW

VOLUME 5 AND ISSUE 14 OF 2025

INSTITUTE OF LEGAL EDUCATION

INDIAN JOURNAL OF LEGAL REVIEW

APIS – 3920 – 0001 | ISSN - 2583-2344

(Open Access Journal)

Journal's Home Page – https://ijlr.iledu.in/

Journal's Editorial Page - https://ijlr.iledu.in/editorial-board/

Volume 5 and Issue 14 of 2025 (Access Full Issue on - https://ijlr.iledu.in/volume-5-and-issue-14-of-2025/)

Publisher

Prasanna S,

Chairman of Institute of Legal Education

No. 08, Arul Nagar, Seera Thoppu,

Maudhanda Kurichi, Srirangam,

Tiruchirappalli – 620102

Phone : +91 73059 14348 - info@iledu.in / Chairman@iledu.in

INDIAN JOURNAL OF LEGAL REVIEW [IJLR – IF SCORE – 7.58]

VOLUME 5 AND ISSUE 14 OF 2025

APIS – 3920 - 0001 *(and)* ISSN - 2583-2344

Published by

Institute of Legal Education

https://iledu.in

THE TECTONIC SHIFT: ARTIFICIAL INTELLIGENCE AND THE EVOLUTION OF CYBERCRIME IN INDIA'S CRIMINAL JUSTICE SYSTEM

AUTHOR – RANJANA* & DR. RANA PARVEEN**

* RESEARCH SCHOLAR AT SCHOOL OF LAW & JURISPRUDENCE, SHRI VENKATESHWARA UNIVERSITY, GAJRAULA (U.P.)

** RESEARCH SUPERVISOR AT SCHOOL OF LAW & JURISPRUDENCE, SHRI VENKATESHWARA UNIVERSITY, GAJRAULA (U.P.)

BEST CITATION - RANJANA & DR. RANA PARVEEN, THE TECTONIC SHIFT: ARTIFICIAL INTELLIGENCE AND THE EVOLUTION OF CYBERCRIME IN INDIA'S CRIMINAL JUSTICE SYSTEM, INDIAN *JOURNAL OF LEGAL REVIEW (IJLR)*, 5 (14) OF 2025, PG. 1107-1114, APIS – 3920 – 0001 & ISSN - 2583-2344. DOI - https://doi.org/10.65393/IKFH6948

Abstract

The rapid convergence of Artificial Intelligence (AI) and the digital economy in India has created a complex web of opportunities and existential threats. As the nation transitions toward a $5 trillion economy, the surge in AI-driven cybercrime—ranging from hyper-realistic deepfakes and automated phishing to sophisticated financial fraud—poses a formidable challenge to the traditional criminal justice framework. This research report provides a multi-dimensional analysis of the escalating cyber threat landscape, the systemic transition from the Information Technology Act of 2000 to the Bharatiya Nyaya Sanhita (BNS) and the Bharatiya Sakshya Adhiniyam (BSA), and the resulting procedural hurdles for law enforcement and the judiciary. Utilising recent data from the National Crime Records Bureau (NCRB) and the Indian Cyber Crime Coordination Centre (I4C), the report highlights a $206% spike in financial losses due to cyber fraud in 2024 alone. It scrutinises the 'black box' problem of AI evidence, the ethical implications of predictive policing, and the critical infrastructure gaps in regional cyber cells. By examining landmark judicial precedents and comparing India's 'hybrid' regulatory approach with the European Union's risk-based model, the study concludes with strategic recommendations aimed at bridging the technical-legal divide through 'accountability by design' specialised institutional training, and a robust framework for digital forensic transparency.

Keywords:

Artificial Intelligence, Cybercrime, Bharatiya Nyaya Sanhita (BNS), Bharatiya Sakshya Adhiniyam (BSA), Digital Evidence, Deepfakes, Financial Fraud, Information Technology Act, Cyber Forensics, India.

The Digital Renaissance and the Dark Frontier: An Introduction

India is currently witnessing a period of unprecedented digital acceleration. With over $86% of households now connected to the internet and the Unified Payments Interface (UPI) processing billions of transactions monthly, the digital landscape has become the primary theatre for both commerce and social interaction.[2215] However, this 'Digital India' renaissance has been shadowed by a rapidly expanding attack surface. The democratisation of Artificial Intelligence (AI) has essentially handed sophisticated weaponry to cybercriminals, enabling the automation of fraud and the creation

[2215] "PIB Headquarters," *available at*: http://www.pib.gov.in/PressNoteDetails.aspx?NoteId=155384 (last visited December 25, 2025).

INDIAN JOURNAL OF LEGAL REVIEW [IJLR – IF SCORE – 7.58]
VOLUME 5 AND ISSUE 14 OF 2025
APIS – 3920 - 0001 *(and)* ISSN - 2583-2344
Published by
Institute of Legal Education
https://iledu.in

of deceptive content on a scale previously unimaginable.

The scale of this shift is reflected in the staggering volume of reported incidents. Cybersecurity incidents in India rose from $ 10.29 lakh in 2022 to $ 22.68 lakh in 2024, representing a significant increase in the complexity of digital threats.[2216] These are not merely individual hacks but often coordinated campaigns by organised crime syndicates, frequently operating from cross-border 'fraud factories' in Southeast Asia. For the average citizen, the threat is no longer a distant theoretical risk but a daily reality manifested in phishing emails, deceptive messages, and 'digital arrest' scams.

The financial toll is equally alarming. In 2024, Indian citizens lost a record ₹ 22,845.73 Crore to cybercriminals, a nearly threefold increase from the previous year's loss of ₹ 7,465 Crore. This surge underscores the efficiency of AI-powered tools in identifying and exploiting human vulnerabilities. As traditional barriers to entry for cybercrime fall—replaced by readily available hacking tools and automated AI scripts—the criminal justice system is forced to grapple with a new paradigm: a world where the perpetrator may not be a human individual, but an autonomous or semi-autonomous algorithm.

Table 1: Escalation of Cyber-Incidents and Financial Losses (2022–2024)

Year	Total Reported Incidents	Year-on-Year Increase	Total Financial Loss (₹ Crore)	National Impact Index
2022	$10,29,026$	$127.44 %	$2,306$	Baseline
2023	$15,96,493$	$55.15 %	$7,465$	High
2024	$22,68,346$	$42.08 %	$22,845$	Critical

Data compiled from.

The nature of these crimes is undergoing a profound transition. Historically, cybercrime was synonymous with data theft or unauthorised access. Today, AI has enabled 'synthetic media' crimes, where deepfakes are used to impersonate high-ranking officials, celebrities, and even family members to facilitate fraud or reputational ruin.[2217] This evolution has rendered colonial-era legal frameworks obsolete, prompting the Indian government to introduce the Bharatiya Nyaya Sanhita (BNS), the Bharatiya Nagrik Suraksha Sanhita (BNSS), and the Bharatiya Sakshya Adhiniyam (BSA) in 2023.[2218]

[2216] Smruti S, "India Lost ₹22,812 Crore to Cyber Fraud in 2024: Report" *Analytics India Magazine*, 2025*available at*: https://analyticsindiamag.com/ai-news-updates/india-lost-₹22812-crore-to-cyber-fraud-in-2024-report/ (last visited December 25, 2025).
[2217] The Hindu Bureau, "AI becoming formidable tool for cybercriminals: Report" *The Hindu*, 25 June 2025, section Bengaluru.
[2218] Record Of Law, "Cybercrime and Digital Policing: Efficacy of the Bharatiya Nyaya Sanhita, 2023" *Record Of Law*, 2025*available at*: https://recordoflaw.in/cybercrime-and-digital-policing-efficacy-of-the-bharatiya-nyaya-sanhita-2023/ (last visited December 25, 2025).

INDIAN JOURNAL OF LEGAL REVIEW [IJLR – IF SCORE – 7.58]
VOLUME 5 AND ISSUE 14 OF 2025
APIS – 3920 - 0001 *(and)* ISSN - 2583-2344
Published by
Institute of Legal Education
https://iledu.in

Mechanisms of AI-Driven Cybercrime: A Modern Taxonomy

To address the challenges faced by the justice system, one must first understand the mechanisms of the crimes themselves. AI is not just another category of crime; it is a 'force multiplier' that changes the origin, mechanism, and outlook of traditional offenses.

The Rise of Deepfakes and Synthetic Identity

Deepfakes—a portmanteau of 'deep learning' and 'fake'—represent the pinnacle of AI misuse in the current era. By training algorithms on existing footage or audio of an individual, criminals can create fabricated media that appears to show the person saying or doing things they never did. In India, the impact has been felt across the political and social spectrum. In 2024, manipulated videos of the Home Minister regarding reservation policies prompted the Election Commission to issue strict guidelines.

Beyond politics, deepfakes have become a tool for 'sextortion' and harassment. Prominent activists and celebrities, such as Ms. Kamya Buch and actors Suniel Shetty and Aishwarya Rai Bachchan, have fallen victim to large-scale harassment campaigns involving pornographic deepfakes and morphed images. The judicial system recognises these acts as violations of the 'right to live with dignity' under Article 21 of the Constitution, yet the ease with which these videos are created and disseminated makes enforcement a game of 'whack-a-mole'.[2219]

Hyper-Personalised Phishing and Social Engineering

Phishing has evolved from generic 'Nigerian Prince' emails to hyper-personalised AI-generated lures. AI tools are now involved in approximately 82.6% of all phishing campaigns, creating messages that mimic the specific writing styles of banks, government agencies, or even colleagues. These campaigns leverage machine learning to bypass standard spam filters and exploit human psychology with alarming precision.

A particularly insidious form of this is the 'pig-butchering' scam—a slow-burn investment fraud where AI is used to maintain long-term digital relationships with victims before siphoning their life savings. These scams are often coordinated from Southeast Asian countries like Cambodia and Myanmar, where human trafficking victims are forced into 'cyber slavery' to run these AI-powered operations targeting Indian citizens.

Automated Malware and Zero-Day Exploitation

On the technical front, AI is being used to find new vulnerabilities in critical infrastructure. Ransomware factions are increasingly targeting Indian corporations, with India leading the regional victim counts for certain malware groups. AI speeds up the process of finding 'zero-day' vulnerabilities—security flaws that are unknown to the developer—thereby driving down the cost of attacks and increasing their frequency.

[2219] "Suniel Shetty vs Ashok Kumar (2025): Deepfake Misuse & Personality Rights Protection in India - J.P. Associates," 2025*available at*: https://jpassociates.co.in/suniel-shetty-deepfake-case/ (last visited December 25, 2025).

INDIAN JOURNAL OF LEGAL REVIEW [IJLR – IF SCORE – 7.58]

VOLUME 5 AND ISSUE 14 OF 2025

APIS – 3920 - 0001 *(and)* ISSN - 2583-2344

Published by

Institute of Legal Education

https://iledu.in

Table 2: AI's Role in Modernising Traditional Cybercrime

Crime Type	Traditional Mechanism	AI-Enhanced Mechanism	Impact on Justice System
Phishing	Generic mass emails	Hyper-personalised, adaptive lures	Difficult to identify patterns
Identity Theft	Stealing passwords/SSNs	Deepfakes and voice cloning	Challenges witness credibility
Fraud	Simple deceptive websites	Automated "pig-butchering" scripts	Massive increase in victim counts
Malware	Pre-written code	Self-evolving, obfuscated malware	Evades signature-based detection

Data synthesised from.

The Legislative Response: Decoding the BNS, BNSS, and BSA

India's primary weapon against technology-based offenses was the Information Technology Act of 2000. While revolutionary at its inception, it was designed for a world of static websites and basic e-commerce. The legislative reform of 2023, which took effect on July 1, 2024, represents a shift toward recognising cybercrime as a central, rather than peripheral, challenge.

Bharatiya Nyaya Sanhita (BNS): Reconceptualizing Accountability

The BNS 2023 replaces the Indian Penal Code (IPC) and introduces several provisions tailored for the digital age. Most notably, Section 2(8) of the BNS expands the definition of "documents" to include electronic and digital records, ensuring that AI-generated synthetic media can be prosecuted under forgery and cheating laws.[2220]

- **Section 319 (Cheating by Personation):** This replaces Section 66D of the IT Act, targeting those who use computer resources to deceive others by pretending to be someone else.
- **Section 336 (Electronic Forgery):** This specifically addresses the creation of fake digital documents or records, which is crucial for tackling deepfake-based misinformation.
- **Section 111 (Organised Crime):** For the first time, the law explicitly targets systematic criminal activities conducted through digital networks, recognising that modern cybercrime is often a corporate-like enterprise.

However, a lingering question remains: can an AI possess *mens rea* (criminal intent)? Under the BNS, accountability is generally assigned to human actors—the developers, manufacturers, or users—rather than the autonomous system itself. This 'tool model' is currently favored in

[2220] Posted on September 29 and 2025 | 12 Min Read, "Deepfakes in India: Legal Landscape, Judicial Responses, and a Practical Playbook for Enforcement" *NeGD - National e-Governance Divisionavailable at:* https://negd.gov.in/blog/deepfakes-in-india-legal-landscape-judicial-responses-and-a-practical-playbook-for-enforcement/ (last visited December 25, 2025).

INDIAN JOURNAL OF LEGAL REVIEW [IJLR – IF SCORE – 7.58]
VOLUME 5 AND ISSUE 14 OF 2025
APIS – 3920 - 0001 *(and)* ISSN - 2583-2344
Published by
Institute of Legal Education
https://iledu.in

India, yet it creates a 'liability gap' when an AI acts in ways its creators did not intend.

Bharatiya Sakshya Adhiniyam (BSA): The Admissibility Challenge

The BSA 2023 replaces the Indian Evidence Act of 1872, modernising the rules for digital evidence. The core of this transition is the replacement of the infamous Section 65B with Section 63 of the BSA.

Under the old regime, Section 65B required a strict certificate for any digital evidence to be admitted. The BSA simplifies this. Section 63(4)(c) still requires a certificate from a 'responsible official' but it eases the technical jargon and focuses more on the chain of custody and the integrity of the record.

Crucially, Section 62 of the BSA now treats certain digital records as 'primary evidence' which can be presented without the rigorous authentication previously required for secondary evidence.[19] This reflects the reality that most modern interactions are 'digital by default'. For example, video recordings that are simultaneously stored and broadcast (like a live social media feed) are now acknowledged as primary evidence.

Table 3: Section 65B (Old) vs. Section 63 (New) of Evidence Law

Feature	Section 65B (Indian Evidence Act)	Section 63 (Bharatiya Sakshya Adhiniyam)
Evidence Category	Usually treated as secondary evidence	Digital records can be primary evidence
Certificate	Mandatory (Anvar and Arjun Panditrao rulings)	Mandatory but simplified in structure
Technical Focus	Focus on machinery and 'regular use'	Focus on authenticity and official responsibility
Flexibility	Rigid; difficult to comply with	Allows for exceptions beyond party control

Data compiled from.

Judicial Precedents and the Protection of Personality Rights

While the legislature drafts the laws, the judiciary has been forced to interpret them in real-time as new AI-driven harms emerge. The Indian courts have been particularly vocal about protecting 'personality rights'—the right of an individual to control the commercial use of their likeness, voice, and persona.

The Suniel Shetty and Karan Johar Rulings

In 2025, the Bombay and Delhi High Courts issued landmark orders protecting celebrities from AI exploitation. In *Suniel Shetty v. Ashok Kumar*, the court addressed the unauthorised creation of deepfake images and voice-cloned audio for false endorsements.[7] The court described the misuse as a 'depraved mind' using technology to invade privacy under Article 21 and infringe upon 'moral rights' under the Copyright Act.[2221]

Similarly, filmmaker Karan Johar secured a

[2221] "Suniel Shetty vs Ashok Kumar (2025): Deepfake Misuse & Personality Rights Protection in India - J.P. Associates," 2025*available at*: https://jpassociates.co.in/suniel-shetty-deepfake-case/ (last visited December 25, 2025).

INDIAN JOURNAL OF LEGAL REVIEW [IJLR – IF SCORE – 7.58]
VOLUME 5 AND ISSUE 14 OF 2025
APIS – 3920 - 0001 *(and)* ISSN - 2583-2344
Published by
Institute of Legal Education
https://iledu.in

restraining order against entities using AI to misuse his name and voice for commercial purposes. These cases have led to the widespread use of "John Doe" orders—injunctions against unknown persons—which allow platforms to take down infringing content without waiting for individual perpetrators to be identified.

The Quest for Constitutional Balance

The judiciary is also aware of the risk of state overreach. In *Shreya Singhal v. Union of India*[2222], the Supreme Court set high standards for content blocking, emphasising that any restriction on digital speech must be necessary and proportionate. When dealing with deepfakes, the courts must balance the need to prevent harm with the 'right of self-incrimination' guaranteed under Article 20(3). For instance, compulsory AI-based lie detection or behavioral mapping could be ruled unconstitutional, similar to the prohibition of narco-analysis in *Selvi v. State of Karnataka*[2223].

The "Black Box" and the Forensic Integrity Gap

Perhaps the most daunting challenge for the criminal justice system is the technical opacity of AI systems—the 'black box' problem. When an AI produces a result (such as a facial recognition match), it often does not provide a human-understandable explanation for *how* it reached that conclusion.

The Challenge of Explainability

In a criminal trial, the standard of proof is 'beyond a reasonable doubt'. If a prosecutor presents AI-generated evidence, the defense has the right to challenge it. However, if the algorithm is proprietary or its logic is too complex for an expert witness to explain, the evidence loses its 'probative value'.[2224] This undermines accountability and can lead to 'automation bias' where judges either blindly trust or blindly reject AI outputs.

Forensic Infrastructure and Backlogs

The physical infrastructure for cyber-investigation in India is struggling to keep pace with the volume of crime. While the government has established the National Cyber Forensic Laboratory (Investigation) in Delhi and Assam, regional cells face severe resource constraints.[2225]

In Madhya Pradesh, for example, over 3 lakh complaints are reportedly pending, with only 230 personnel adequately trained to handle cyber-complexities.[2226] This backlog means that by the time a case is investigated, the digital evidence may have been overwritten or lost, effectively granting immunity to the perpetrator. In contrast, Uttar Pradesh has taken a phased approach, training over 84,000 personnel through a dedicated portal and establishing cybercrime stations in all 75 districts.[2227]

Institutional Innovation: The Role of IIT Kanpur and I4C

To fight fire with fire, the Indian government has partnered with academic and technical institutions to develop indigenous AI solutions for law enforcement.

IIT Kanpur's AIIDE Centre of Excellence

The Artificial Intelligence and Innovation Driven Entrepreneurship (AIIDE) Centre of Excellence (CoE) at IIT Kanpur is a critical hub for this effort. Incubated startups like the Future Crime Research Foundation (FCRF) are developing 'predictive policing' tools that map crime hotspots to help police allocate resources more

[2222] AIR 2015 SC 1523.
[2223] 2010 (7) SCC 263.
[2224] Aayushman Verma, "Accountability By Design: Shared Liability In AI Fraud Under Indian Cyber Law | Virtuosity Legal," 2025*available at*: https://virtuositylegal.com/accountability-by-design-shared-liability-in-ai-fraud-under-indian-cyber-law/ (last visited December 25, 2025).
[2225] "SCHEME FOR CAPACITY BUILDING TO CONTROL CYBER CRIMES,"*available at*: https://www.pib.gov.in/www.pib.gov.in/Pressreleaseshare.aspx?PRID=2198260 (last visited December 25, 2025).
[2226] Deepak Sahu, "Cybercrime Crisis: MP Cell Faces Massive Backlog" *https://www.facebook.com/VARINDIAMagazineavailable at*: https://www.varindia.com/news/cybercrime-crisis-mp-cell-faces-massive-backlog (last visited December 25, 2025).
[2227] "UP trains over 84k police personnel to tackle rising cybercrime | Hindustan Times,"*available at*: https://www.hindustantimes.com/cities/lucknow-news/up-trains-over-84k-police-personnel-to-tackle-rising-cybercrime-101766499788981.html (last visited December 25, 2025).

INDIAN JOURNAL OF LEGAL REVIEW [IJLR – IF SCORE – 7.58]
VOLUME 5 AND ISSUE 14 OF 2025
APIS – 3920 - 0001 *(and)* ISSN - 2583-2344
Published by
Institute of Legal Education
https://iledu.in

efficiently.[2228]

Another notable innovation is 'SecureTrace' a blockchain forensic platform designed to trace illicit cryptocurrency transactions in real-time across multiple blockchains. This is essential for tackling the rising trend of crypto-based scams and ransomware payments, which traditional bank tracing cannot follow.

The Indian Cyber Crime Coordination Centre (I4C)

Under the Ministry of Home Affairs, the I4C serves as the nerve center for national cyber-response. Key initiatives include:

- **National Cyber Crime Reporting Portal (NCRP):** Allows citizens to report incidents instantly, leading to the blocking of over 9.42 lakh SIM cards and 2.6 lakh IMEIs linked to fraud.
- **CFCFRMS (1930 Helpline):** A real-time system that has saved more than $₹5,489$ Crore by freezing fraudulent transactions before the funds are siphoned off.
- **Pratibimb Module:** A tool that maps the geographic location of cybercriminals and their infrastructure, allowing jurisdictional officers to see exactly where the threats are originating.

Comparative Governance: India vs. The EU AI Act

As India formulates its own AI strategy, it is useful to look at the global gold standard: the EU AI Act (2024). The EU employs a 'risk-based' framework, classifying AI into four categories of risk and banning those that pose an 'unacceptable risk' such as social scoring or untargeted facial recognition in public spaces.[2229]

India's approach is currently more 'hybrid'. While it values innovation and does not want to stifle the start-up ecosystem, it is increasingly moving toward a 'rights-based' model for high-risk applications like criminal justice. The Digital Personal Data Protection (DPDP) Act of 2023 adds a layer of accountability, mandating user consent for data processing and imposing fines of up to $₹250$ Crore for breaches.

However, unlike the EU, India does not yet have a dedicated 'AI Act'. Instead, it is 'stretching' existing laws (BNS, IT Act) to fit novel AI scenarios. This creates legal uncertainty: is an AI a 'product' (product liability), an 'agent' (vicarious liability), or a 'person' (direct liability)?.

The Human Factor: Cyber Slavery and Victim Demographics

The criminal justice system must also account for the sociological shifts caused by AI. Cybercrime is no longer just about 'thugs' in a basement; it has international human rights implications.

The 'Cyber Slavery' Crisis

A significant portion of cyber-fraud targeting India originates from Southeast Asia. Indian nationals are often lured to countries like Cambodia and Myanmar with promises of high-paying tech jobs, only to have their passports seized and be forced to conduct scams. This creates a complex legal scenario: the person making the fraudulent call is himself a victim of trafficking. Data from the Bureau of Immigration shows that over 29,000 Indian nationals who travelled to these regions between 2022 and 2024 have not returned, highlighting the scale of this 'double-impact' crisis.

Vulnerable Populations

AI allows criminals to target specific demographics with 'precision scams'. Senior citizens are frequently targeted with 'digital arrest' frauds, while women and children are victims of AI-generated harassment and bullying. For example, in Karnataka, cybercrime

[2228] The420 Web Desk, "IIT-Kanpur Incubates FCRF For Developing First-Of-Its-Kind AI-Powered Search Engine For Predictive Policing & Crime Mapping" *The420.in*, 2022*available at*: https://the420.in/iit-kanpur-incubates-fcrf-for-developing-first-of-its-kind-ai-powered-search-engine-to-help-smoothen-policing-process/ (last visited December 25, 2025).

[2229] Dr. Girijarani Reddy, "Regulating Artificial Intelligence: A Critical Analysis of Emerging Legal Frameworks in India, EU, and the USA," 12 *International Journal of Academic Research* 102–5 (2025).

INDIAN JOURNAL OF LEGAL REVIEW [IJLR – IF SCORE – 7.58]
VOLUME 5 AND ISSUE 14 OF 2025
APIS – 3920 - 0001 *(and)* ISSN - 2583-2344
Published by
Institute of Legal Education
https://iledu.in

cases in rural areas nearly doubled between 2022 and 2024, as digital literacy lags behind digital access.

Layman's Analogies: Understanding AI in the Courtroom

To explain these complex concepts to a layman or a jury, experts often use analogies. These help demystify the 'magic' of AI and ground it in familiar territory.

1. The Rockets and Planes Analogy

Think of AI as a rocket. To build a successful rocket, you need fuel (Data), materials (Hardware/Software), and skilled engineers (Data Scientists). Cybercrime happens when someone builds a 'malicious rocket' to crash into a digital city. The justice system's job is to identify who provided the fuel and who designed the engine.[2230]

2. The Chef and the Cookbook

Generative AI (like deepfake tools) is like a master chef who has memorised every recipe in the world (the Dataset). When someone asks for a specific 'dish' (a prompt for a fake video), the chef doesn't just copy an old recipe; he creates a completely new dish based on his knowledge. The 'crime' occurs when the chef is asked to cook something poisonous—like a video that ruins someone's reputation.[2231]

3. Sneakers, Steroids, and Coaches

In terms of using AI in the judiciary or police:

- **Steroids:** Elevate performance quickly but leave you worse off in the long term (e.g., over-relying on automated profiling without checking the facts).
- **Sneakers:** Give you a temporary boost to work faster without changing your skill level (e.g., using AI to transcribe files).
- **Coaches:** Help you improve your own human capabilities over time (e.g., AI that highlights inconsistencies in a case file for a human judge to review).[2232]

Conclusions: The Road Ahead for Digital Justice

The integration of Artificial Intelligence into the cybercriminal landscape has permanently altered the trajectory of the Indian criminal justice system. The move from colonial-era codes to the BNS and BSA represents a bold and necessary modernisation. However, legislation is only the first step. The ultimate efficacy of these laws depends on the simultaneous growth of technological infrastructure, personnel capacity, and forensic explainability.

The 'Cyber Fraud Epidemic' with its $₹22,845$ crore annual loss, is a signal that the traditional 'reactive' policing model is insufficient. The future of justice in India must be 'proactive'. It must leverage AI to detect fraud in real-time while maintaining strict "human-in-the-loop" supervision to protect constitutional rights.

As AI continues to evolve, the distinction between authentic and fabricated digital evidence will become even thinner. The criminal justice system must therefore become a 'technological gatekeeper' ensuring that the tools used to provide justice do not themselves become instruments of bias or error.

Recommendations for a Comprehensive AI-Cybercrime Strategy

To build a resilient and fair criminal justice system in the age of AI, the following multi-stakeholder recommendations are proposed:

1. Institutional and Forensic Strengthening

- **Establish Specialised AI Forensic Labs:** Every state should have a dedicated facility for 'algorithmic auditing' and 'synthetic media verification' moving beyond simple data extraction to true AI-forensics.
- **Bridge the Talent Gap:** The government

[2230] "Two Useful Analogies for Understanding and Working With AI," *Sysabeeavailable at*: https://www.sysabee.com/index.php/articles/two-useful-analogies-for-understanding-and-working-with-ai/ (last visited December 25, 2025).

[2231] "Where might AI lead us? An analogy offers one possibility," 2024*available at*: https://cte.ku.edu/where-might-ai-lead-us-analogy-offers-one-possibility (last visited December 25, 2025).

[2232] Jake Hofman, Daniel G. Goldstein and David Rothschild, "A Sports Analogy for Understanding Different Ways to Use AI" *Harvard Business Review* (2023).

must scale the 'Cyber Commando' and 'CyTrain' programs, aiming to train not just 84,000 but the entire million-strong law enforcement workforce in AI-specific investigation.

- **Mandatory Explainability:** For any AI-generated forensic report to be admissible in court, it must be accompanied by an 'Explainability Certificate' that details the training data used and the algorithm's error rates.

2. Legislative and Regulatory Updates

- **Dedicated AI Liability Statute:** Resolve the 'black box' accountability gap by enacting a law that defines shared liability for developers, deployers, and users of AI systems.
- **Standardised Digital Certificates:** Standardise the Section 63(4)(c) certificate under the BSA to ensure it includes metadata and forensic hashes that can be verified by independent third-party experts.
- **Update Intermediary Guidelines:** Require social media platforms to implement 'Digital Watermarking' and 'Proactive Deepfake Detection' tools, removing harmful synthetic content within a strict 36-hour window.

3. Judicial and Constitutional Safeguards

- **Judicial Training on 'Automation Bias':** National and State Judicial Academies must introduce curricula on 'Digital Evidence Evaluation' to help judges understand the limitations and biases of AI tools.
- **Establish 'Digital John Doe' Protocols:** Create a streamlined, pan-India protocol for "John Doe" orders to ensure that victims of AI-harassment can get content removed across multiple platforms with a single court order.
- **Constitutional Audit of Predictive Policing:** Before deploying AI for 'crime mapping' or 'surveillance' a constitutional impact assessment should be mandated to ensure compliance with Article 21 (Right to Privacy).

4. Public Awareness and International Cooperation

- **Digital Literacy as a Fundamental Skill:** Incorporate "Cyber Hygiene" and "AI Awareness" into school curricula and workplace training, focusing on the detection of deepfakes and phishing.
- **Fast-Track "Digital MLATs":** India should collaborate with G20 and OECD partners to create a "Fast-Track Digital Treaty" for the real-time sharing of cyber-evidence, particularly focusing on Southeast Asian fraud hubs.
- **Accountability by Design:** Encourage start-ups and corporations to adopt "Ethical AI" principles from the design stage, ensuring that transparency and fairness are built into the code, not added as an afterthought.

By implementing these measures, India can ensure that its criminal justice system remains a robust protector of order and rights in an increasingly automated world. The goal is not to stop technological progress, but to ensure that progress is synonymous with justice.