TECHNOLOGY AS A DOUBLE-EDGED SWORD IN MODERN CRIMES: AN INDIAN PERSPECTIVE

Navya Singh, Siddhartha Law College, Dehradun

ABSTRACT

Technology has drastically changed crime and criminal justice in India. Law enforcement agencies can now use advanced tools like AI-enabled surveillance systems, digital forensics, predictive policing tools and others on one hand. On the other hand, its efforts have also upgraded crooks with deepfakes, crypto laundering channels, UPI exploitation techniques and dark web facilities to commit more and more offences that are hard to detect, investigate and prosecute. This paper analyses the double-edged sword of technology as observed in modern crimes in India. The data set is taken from the National Crime Records Bureau (NCRB). There has been a legislative development through the introduction of the Bharatiya Sakshya Adhiniyam, 2023. This also serves as the background for the study of the latest cases of deepfake scams and digital arrest fraud. India's preparation for the cyber-digital war has reportedly improved since 2020. Nonetheless, the still unrepaired deficiencies in skilled manpower and the legal admissibility protocol, conviction rates and privacy safeguards have hampered the effectiveness of technology as a crime-fighting tool. The recommendations in the paper advocate for a balanced, rights-respecting use of technology in the Indian criminal justice system.

INTRODUCTION

Nothing short of remarkable, India has seen a lot of evolution in the digital space. India achieved a lot in the digital space, it is nothing short of amazing! With nearly 900 million users of the internet and one of the world's largest populations, the Asian country has seen the adoption of technology in governance, business, education and more. India is swiftly transforming into a modern digital economy. UPI witnesses billions of transactions on a monthly basis and Digital India is also steering the country in this way.

Nonetheless, connectivity has become a medium for a new breed of crimes. India is rapidly morphing into a modern digital economy. Billions of transactions happen through UPI every month and Digital India is also driving the country in this direction.

However, connectivity has become a means of a new generation of crimes.

Scholars have long observed that Technology "is always a double-edged sword and can be used for both the purposes-good or bad" by Sharma (2020). This is evident in the Indian context. The increasing usage of technology in the law enforcement domain has become necessary to cope up with delinquent activities. Indian police are solving cases faster with the help of the Indian Cyber Crime Coordination Centre (I4C), AI-powered CCTV networks and digital forensic labs.[1] Fraud is now occurring in the same environment. For instance, a deepfake of a stock market official. With the use of encrypted messages, the banks are fooled Complicated techniques to spoof UPI security. In the same environment, fraud has started happening. For example, a deepfake created to impersonate a stock exchange official. Use of encrypted messages to fool banks. Using complicated methods to bypass UPI security.

The Indian context is reviewed in regard to both aspects of this phenomenon. It first demonstrates how technology aids in perpetrating crimes, then examines how technology is used to prevent and detect crimes, before finally looking at the legal, institutional and ethical dilemmas posed.

[1] Press Information Bureau, Government of India, Curbing Cyber Frauds in Digital India (2025), https://www.pib.gov.in/PressReleasePage.aspx?PRID=2176146.

TECHNOLOGY AS A FACILITATOR OF MODERN CRIMES IN INDIA

➢ THE ALARMING RISE OF CYBER CRIMES

The statistical course of cybercrime in India is alarming. As per the data released by NCRB in its report Crime in India the total number of registered cybercrime cases in India rose from 52,974 in 2021 to 65,893 in 2022 and increased to 86,420 in 2023, representing an increase of more than 63 % in just two years .[2]

States like Karnataka (21,889 incidents), Telangana (18,236 incidents), Uttar Pradesh (10,794 incidents), and Maharashtra (8,103 incidents) were among the worst-affected states in 2023.[3] This is believed to be only a fraction of the reality, as many cybercrimes go unreported.

Law enforcement statistics are alarmingly low. According to NCRB data (Kaushik, 2025), out of 31,584 persons who were charge-sheeted in cybercrime cases in 2023, just 1,104 were convicted, with a conviction rate of about 3.5 per cent.[4]

The gap between rising cases and static convictions highlights the difficulties faced by law enforcement in a changing technological environment.

➢ DEEPFAKES, DIGITAL ARRESTS AND AI- ENABLED FRAUDS

The criminal use of artificial intelligence, often in weapons, is the most concerning issue. Deepfake technology, which creates realistic fake videos, audio and images using artificial intelligence, has become a tool for financial fraud in India. In early 2026, a deepfake video of the Chief Executive of the Bombay Stock Exchange (BSE), Sundararaman Ramamurthy surfaced on social media, in which he allegedly gave stock-buying advice to investors. The video was completely made up. As quoted in Long and Butler (2026), Ramamurthy said that it was something that people would have access to in the public domain and got cheated into buying or selling stocks as

[2] Press Information Bureau, Government of India, Cyber Crime Cases (Mar. 17, 2026), https://www.pib.gov.in/PressReleasePage.aspx?PRID=2241339.
[3] National Crime Records Bureau, Ministry of Home Affairs, Crime in India 2023: Statistics (2025), https://www.ncrb.gov.in/crime-in-india-year-wise.html?year=2023.
[4] Press Information Bureau, Government of India, Cyber Crime Police Stations (Mar. 11, 2026), https://www.pib.gov.in/PressReleasePage.aspx?PRID=2238253.

though I recommended them. AI scams are becoming more common and widespread in India. A 2025 analysis found that 47% of Indian adults say they either have been or know someone who has been a victim of AI scams (Observer Research Foundation, 2026).

The unreasonable arrests in the virtual space are an alarming phenomenon. Fake law enforcement video calls using deepfake technology report victims. In legal matters, criminals fraudulently compel victims to transfer money using threats and intimidation. These cons take advantage of both technological sophistication and the public's fear of authority.

- **UPI EXPLOITATION AND FINANCIAL CYBERCRIMES**

The UPI system in India became victims of cybercrime despite many revolutionary features. Media reports from 2026 reveal that fraudsters are leveraging new technology to breach UPI security to make financial transactions. The techniques being used include OTP interception, application exploitation and SIM-swap frauds (Economic Times BFSI, 2026). The great ability of UPI is that it is instantaneous and real-time. But this is also its weakness as this can be exploited. In other words, scam transactions could be instantaneous and permanent.

- **THE DARK WEB, CRYPTOCURRENCY, AND ORGANISED CRIMES**

The dark web is basically an anonymous online marketplace filled with drugs, weapons, counterfeit currency, and stolen personal data. According to news reports, India's law enforcement agencies are experiencing an increase in cases of money laundering involving cryptocurrency. Criminal syndicates are increasingly employing these methods, which render the law enforcement agencies incapable of tracing the tainted money easily. Blockchain technology's decentralised and pseudonymous features have brought about legitimate benefits, but also provide criminals with a sophisticated means of concealing their proceeds.

- **CRIME AGAINST WOMEN IN THE DIGITAL SPACE**

The advances in technology have also been misused to carry out crimes against women. The Centre for Public Policy Research states that online crimes against women have

risen to 48,475 in 2024 compared to 22,188 in 2020. The increase in percentage is around 118.4 percent. The anonymity of these platforms allows the perpetrators to commit these crimes more freely, while on the other hand, victims face great trouble in reporting these crimes and getting justice.

TECHNOLOGY AS A TOOL FOR CRIME PREVENTION AND DETECTION

➢ DIGITAL FORENSICS AND NATIONAL FORENSICS INFRASTRUCTURE

India has made substantial investments in building digital forensic capacity since 2020. The Indian Cyber Crime Coordination Centre (I4C), operational under the Ministry of Home Affairs, serves as the national nodal agency for cybercrime prevention.

Major institutional support systems are: -

- The National Cyber Forensic Laboratory (Investigation) unit in New Delhi has supported 11,800 plus cases thus far with real time forensic assistance to state investigating officers.
- The National Cyber Forensic Laboratory (Evidence) was set up in 2022 at Hyderabad and has been able to decrease the forensic turnaround time by almost 50% through its imaging, malware analysis, and decryption tools.
- There are seven Central Forensic Science Laboratories (CFSLs) and 27 State Forensic Science Laboratories operating in the country that are connected through a national e-Forensics IT platform that integrates more than 117 labs.

The Ministry of Home Affairs has allocated ₹116.5 crore as financial assistance under the Cyber Crime Prevention against Women and Children (CCPWC) scheme. This assistance has been given to the States and UTs for setting up of cyber forensic-cum-training laboratories which have been set up in 33 States/UTs,[5] more than 550 mobile forensic vans are available at the district level for data extraction at remote locations.

[5] Press Information Bureau, Government of India, Digital Transformation of Justice: Integrating AI in India's Judiciary and Law Enforcement (2025), https://www.pib.gov.in/PressReleasePage.aspx?PRID=2106239.

➢ AI IN POLICING AND SURVEILLANCE

The technology has empowered criminals; it has empowered those fighting crime. To enhance crime detection, surveillance, and investigation, the Government of India is integrating Artificial Intelligence in law enforcement. One of the suggested applications of AI is para predictive policing, where AI models can look at crime, high-risk areas, and behaviour. Another use case includes facial recognition software connected to the national criminal database, application of AI tools in forensic investigation to study evidence and digital footprints, and automating drones to surveil crime scenes and track suspects. [6]

The Crime and Criminal Tracking Network System (CCTNS), having integrated with e-Prisons and e-Forensics databases, will leverage the power of AI and help with data-driven crime tracking and intelligence. According to PIB (2025a), there is a growing upgrade by Indian law enforcement agencies of current CCTV installations to AI-enabled ones, which assist police with real-time monitoring and alerting in crime detection and prevention.[7]

➢ DIGITAL FORENSICS AND ELECTRONIC EVIDENCE

Digital forensics has transformed investigation practices. Digital Footprints are the traces left behind by users while they use Internet. The accumulation, storage, and analysis of digital footprints reconstruct events, identify suspects and prove intent. The admissibility of electronic evidence in India is regulated by the Information Technology Act, 2000, and Section 65B of the Indian Evidence Act, 1872 (now Bharatiya Sakshya Adhiniyam, 2023). In the Supreme Court case Anvar P.V. v. P.K. Basheer, established the necessity of compliance with Section 65B for the admissibility of electronic records.

➢ INSTITUTIONAL MECHANISM

India has established many institutional mechanisms to curb cybercrimes. I4C is the Indian Cyber Crime Coordination Centre set up in 2018 under the Ministry of Home Affairs as the nodal body to coordinate responses to cybercrime. The capability to

[6] Ibid.
[7] Ibid.

report cybercrime has been provided with the NCRP. According to a news update in 2025 by The Times of India, the application, CFCFRMS (Citizen Financial Cyber Fraud Reporting and Management System), has saved over ₹5,489 crore from a total of 17.82 lakh complaints as it enables quick freezing and recovering of stolen money. Furthermore, the 'Pratibimb' module maps networks of cybercriminals across geographical spheres, leading to 10,599 arrests and 26,096 criminal linkages. According to The Times of India 2025, the Centre has blocked more than 942823 SIM cards, and what's more, blocked 263796 IMEI numbers related to cyber fraud.

- **AI IN THE JUDICIARY**

The government has allocated ₹7,210 crore for the Phase III of e-Courts Project, which will utilize artificial intelligence (AI) for automatic case management, legal research, AI-assisted filing, virtual legal assistants, and case outcomes prediction (PIB, 2025a). AI-powered legal translation systems are overcoming language obstacles in a courtroom system which predominantly functions in English, simplifying access to justice for non-English-speaking litigants. The High Court of Kerala in July 2025 became the first state to adopt a formal policy on the use of AI tools in the district judiciary (Oxford Institute of Technology and Justice, 2025).

LEGAL AND REGULATORY FRAMEWORK

- **THE INFORMATION TECHNOLOGY ACT, 2000**

The Information Technology Act of 2000 is India's primary law on cybercrimes and electronic commerce. A crucial provision is Section 65 (tampering with a computer source document), Section 66 (hacking), Section 66C (identity theft), Section 66D (cheating by personation using computer resource), section 66E (violation of privacy), Section 67 (publishing or transmitting obscene material in electronic form), and Section 66F (cyber terrorism – penalty life). In 2008, the Act was amended to include child pornography, voyeurism, terrorism, and other cybercrimes related to pornography. People have critised the act because they believe most of the offences are bailable. Hence, it does not act as a very effective deterrent (Jayashree et al, 2025).

- **THE NEW CRIMINAL LAW REFORMS**

In 2023, India established three new criminal codes replacing the colonial professional Indian Penal Code, Evidence Act and Criminal Procedure Code.

The 2023 Bharatiya Nyaya Sanhita makes illegal identity theft, impersonation and organized crime. As per Section 318(4) of the BNS (which takes the place of Section 420 of the IPC), "cheating and dishonestly inducing delivery of property" is defined. Sections 335–340 deal with forgery of an electronic document. According to the CyberPeace Foundation (2026), the Bharatiya Sakshya Adhiniyam, 2023 (which would replace the Indian Evidence Act), lays down the framework for the proof of electronic records.

- **THE DIGITAL PERSONAL DATA PROTECTION ACT, 2023**

This Act provides a comprehensive framework for the protection of personal data, mandating informed consent for data collection and imposing obligations on data fiduciaries. It is particularly relevant in an era when AI-generated deepfakes and identity theft exploit vast repositories of personal data.

GAPS AND CHALLENGES

There are still major gaps not yet covered. India does not have legislation specific to deepfakes, and hence crimes are managed under the general provisions of the IT Act, which are not prepared for challenging the unique use of synthetic media. Police and judicial officers are often inadequately trained in the investigation of cybercrime and digital evidence. We still have weak coordination between law enforcement and technical agencies. Our cyber forensic infrastructure is weak, especially in smaller states and rural areas. Cross-border cybercrime cases are extremely complicated jurisdictionally (Statista Research Department, 2025).

BALANCING THE DOUBLE-EDGED SWORD

There is ample evidence to show how technology can be a boon or a bane for crimes in India. Nonetheless, India's rapid digitalisation partly through UPI, partly Aadhaar and mobile banking has subjected a large section of the population to cyber fraud, deep fake scam and use of AI to facilitate crime. On the contrary, the same technologies, e.g. Advanced technologies

including AI, digital forensics, predictive policing and blockchain can aid crime detection, prevention and prosecution. Indian policymakers face a big question: how to maximize the usage of technology and minimize their abuse.

CrowdStrike's head of counter adversary operations Adam Meyer, aptly described AI as a double-edged sword and cited how agentic AI could greatly improve the defender's efficiency. But, a surge in threats of such magnitude is anticipated, as zero-day vulnerabilities would be found at a great pace through AI, and their cost would lower making them easily available to criminals (The Economic Times, 2025).

India's institutional response is multi-layered. The response consists of the IT Act, the new criminal codes, I4C, CERT-In, and NCRP. Together these provide an important foundation. As cybercrime evolves at a speed more than the legislation, we need dynamic progressive law.

CONCLUSION

Technology in present India is undoubtedly a double-edged sword. Access to information finance and governance has been democratized but on the other hand it has also empowered criminals with the tools of deception fraud exploitation at an unparalleled scale. In 2023, cybercrime statistics have risen from 27,248 in 2018 to 86,420. Financial losses of ₹22,845 crore in 2024 really makes this challenge serious. At the same time, India's deployment of AI in police, digital forensics, and judiciary is strong evidence that the technology is the best counter of technolgoically driven crime.

The answer is not to restrict technologies. The answer lies in creating legal, institutional and educational frameworks which can cope with the pace of change in technology, crime and its counter-measure. India's experience shows that with digitization, the governance of technology matters will also become as crucial as technology.

REFERENCES

1. Centre for Public Policy Research, Online Crimes Against Women in India: Deepfakes, Doxxing, and Digital Abuse, Ctr. for Pub. Pol'y Rsch. (2025), https://www.cppr.in/articles/deepfakes-doxxing-and-digital-abuse.

2. CyberPeace Foundation, The Data Behind India's Digital Fraud Surge, CyberPeace Found. (2026), https://www.cyberpeace.org/resources/blogs/the-data-behind-indias-digital-fraud-surge.

3. Prithvi Jainendran, Deepfakes and Financial Cybercrime: India's Multi-Layered Response, Observer Rsch. Found. (2026), https://www.orfonline.org/expert-speak/deepfakes-and-financial-cybercrime-india-s-multi-layered-response.

4. J. Jayashree et al., Deepfake Cyber Threats in India: An Emerging Challenge Without Legal and Technical Safeguards, Int'l J. Eng'g Rsch. & Tech. (2025), https://www.ijert.org/deepfake-cyber-threats-in-india-an-emerging-challenge-without-legal-and-technical-safeguards-ijertconv14is010082.

5. Oxford Institute of Technology and Justice, India: Increasing Use of AI Across the Justice System (2025), https://www.techandjustice.bsg.ox.ac.uk/research/india.

6. Press Information Bureau, Government of India, Digital Transformation of Justice: Integrating AI in India's Judiciary and Law Enforcement (2025), https://www.pib.gov.in/PressReleasePage.aspx?PRID=2106239.

7. Press Information Bureau, Government of India, Curbing Cyber Frauds in Digital India (2025), https://www.pib.gov.in/PressReleasePage.aspx?PRID=2176146.

8. Statista Research Department, Cyber Crime in India – Statistics & Facts, Statista (2025), https://www.statista.com/topics/5054/cyber-crime-in-india/.

9. AI-Driven Cybercrime Threatens India's $5 Trillion Dream, Econ. Times (Oct. 27, 2025), https://m.economictimes.com/tech/artificial-intelligence/ai-driven-cybercrime-threatens-indias-5-trillion-dream/articleshow/124834185.cms.

10. India's Cyber Fraud Epidemic: Rs 22,845 Crore Lost in 2024; 206% Jump from Previous

Year, Says Government, Times India (July 22, 2025), https://timesofindia.indiatimes.com/business/cybersecurity/indias-cyber-fraud-epidemic-rs-22845-crore-lost-in-just-a-year-206-jump-from-previous-year-says-government/articleshow/122840099.cms.