

AI Driven Document Forgery as a National Security Threat: A Critical Examination of Data Mining and the Right to Privacy

Dharmendra Panwar^{1*} | Dr. K R Meghwal²

¹Ph.D. Research Scholar, Department of Law, JNVU Jodhpur, Rajasthan.

²Assistant Professor of Law, Faculty of Law, JNVU Jodhpur, Rajasthan.

*Corresponding Author: dharmendra11panwar@gmail.com

Citation: Panwar, D. & Meghwal, K. (2026). AI Driven Document Forgery as a National Security Threat: A Critical Examination of Data Mining and the Right to Privacy. *International Journal of Advanced Research in Commerce, Management & Social Science*, 09(02(IV)), 198–203. [https://doi.org/10.62823/IJARCMSS/9.2\(IV\).9405](https://doi.org/10.62823/IJARCMSS/9.2(IV).9405)

ABSTRACT

Indian national security architecture has undergone a radical, irreversible change over the past decade. Traditional threats, mainly resulting from physical penetration, armed rebellion, and traditional espionage, have been combined with technologically advanced means that exploit digital infrastructure. Artificial intelligence has become a dual-use technology that will improve the efficiency of governance while, at the same time, providing hostile parties with unprecedented means of deception. The creation of hyper-realistic identity credentials, financial instruments, immigration documents, and biometric records that can circumvent traditional verification systems is among the gravest manifestations of this development, as they can be used to forge documents and advance criminal activities (AI-driven document forgery). The boosted digitisation of welfare distribution, banking, electoral registration, taxation, and health services in India has created a large storage of personal data and digital credentials. Although this change has made the administration more transparent and inclusive, it has also created a larger attack surface for bad actors. The latest statistical data for 2024-2026 show a drastic increase in the number of cybercrime complaints, losses in the tens of thousands of crores, and rapid growth in synthetic identity fraud enabled by generative artificial intelligence. The paper critically explains whether the emerging legal framework in India which embraces the Information Technology Act, 2000, the Bharatiya Nyaya Sanhita, 2023, the Digital Personal Data Protection Act, 2023, and the Unlawful Activities Prevention Act, 1967 have adequately prepared to take on the evolving document forgery in India-based on AI technology without compromising the provisions of privacy as expressed in the Justice K S Puttaswamy v Union of India. This paper argues, through an analytical examination of geopolitical processes, transnational scam networks, state-sponsored cyber activities, and domestic responses, that AI-driven forgery is a hybrid threat to national security and that a techno-legal response should be carefully calibrated. The main dilemma is how to balance the increased data mining and surveillance with the proportionality requirement of the constitutional jurisprudence.

Keywords: Artificial Intelligence, Constitutional Law, Data- Protection, Technology, National Security.

Introduction

Digital Threat Statistical Landscape 2018 to 2026

The growth of online governance and business in India over the past three to four years (since 2018) has been accompanied by a parallel rise in cyber-related crimes, with both the number and character of these crimes increasing. The growing use of online payments, biometric authentication, online documentation, and paperless administrative processes has gone a long way toward eliminating friction in economic and social dealings. Nevertheless, it is the same infrastructure that has exposed

gaps, which are now actively used by organised criminal syndicates and aggressive actors who can cross jurisdictional boundaries. Data published by the law enforcement agencies via the National Cyber Crime Reporting Portal and the number of cases of reported cyber incidents indicate that the number of reported cases of cybercrimes has increased over the years, with 10.29 lakh in 2022 to over 22.68 lakh in 2024, signifying an alarming change in awareness and criminal activity.¹ Economic damage has also been widespread, and the loss in 2024 was reportedly more than 22,845 crore, almost three times the amounts reported in the prior three years.²

This statistical run-up should be explained in the context of the evolving nature of cyber offences. Initial forms of digital fraud included high-volume phishing emails, SMS-based fraud, and simple identity fraud using stolen documents. Modern-day fraud, however, is increasingly driven by generative artificial intelligence, which can create high-resolution forged identity documents that can withstand shallow investigation. Deepfake technology is a technology that allows the generation of fake video and audio recordings that convincingly imitate the voices and faces of actual people. When used in the context of financial crime, these tools enable fraudsters to masquerade as bank, police, or government officials in real-time communications. In early 2025, it was reported that there had been a drastic increase in deepfake-based identity attempts, with some sectors experiencing growth of over 200% compared to the previous year.³

This is evidenced by the fact that the digital arrest scam is described in popular terms as rather sophisticated. The victims are contacted by individuals who claim to be investigative officers and state that the target's identity has been linked to a crime. Victims are intimidated into sending money through the threat of being arrested by using fabricated warrants, fake documents, and imitated voices. Such scams are usually based on personal information collected due to an existing breach or purchased at illegal online auctions. Data mining and AI-based forgery are also more credible, making it harder for ordinary citizens to detect.

The Global Cybersecurity Outlook 2026 highlights the seriousness of this change by listing AI-related vulnerabilities among the most proliferating threats to national security worldwide. A large percentage of cybersecurity professionals surveyed emphasised synthetic identity fraud and AI misinformation as the main threats. In India, where a digital identity is used to verify beneficiaries of welfare programs, financial inclusion, and voters, the consequences are especially grave. The statistical landscape thus shows not only an increase in crime but also a shift in structure, reflecting a transformation in the character of the threats facing the state.⁴

Hybrid Threats and Regional Geopolitics

India's digital vulnerability cannot be understood outside a geopolitical context. A combination of technological capabilities, cross-border networks, and strategic competition has resulted in hybrid threats that combine cyber operations, economic crime, and ideological extremism.⁵ AI-facilitated document forgery can often operate within this larger matrix, facilitating infiltration, funding, and espionage.

- **Identity and Terror Axis: Pakistan and Bangladesh:** The eastern and western borders of India have traditionally been places of migration, conflict, and illicit trade. In previous decades, infiltration had to involve physical crossing guarded frontiers. The goal now is not only to cross the border but also to become integrated into the digital identity ecosystem of the Indian state. Voter identification cards, forged Aadhaar credentials, and other government-issued documents grant access to banking systems, tele-communications services, and government benefits. The intelligence tests have indicated that some cross-border networks are enabling identity laundering, in which individuals obtain or create Indian records through intermediaries working in border districts.⁶

In the eastern corridor, weak political environments and socioeconomic conditions have at times provided fertile ground for transnational criminal cooperation. Narcotics or counterfeit currency networks that have previously specialised in smuggling have now adopted digital forgery services. Generative AI tools do not require physical printing presses or specialized counterfeit workshops, as they can be used. Rather, personal information in digital templates enables the quick creation of convincing papers that can be delivered electronically.

The history of Pakistan being put under the microscope in issues of terror financing is another cause of concern. The informal systems of value transfer that frequently operate outside formal banking

systems can be complemented by accounts created using forged digital identities.⁷ Minor value transfers, when repeated across several accounts, can perpetuate extremist networks. The AI-based documentation is therefore a force multiplier that will make it difficult to monitor financial intelligence. The shift from physical intrusion to a digitally embedded platform is one of the strategic re-adjustments, where aggressive actors aim to take advantage of the transparency of India's digital governance model.

- **State-Sponsored Cyber Espionage: China:** The strategic rivalry between India and China is going on even in cyberspace, with claims of state-sponsored cyber campaigns becoming common. Indian authorities have reported hundreds of millions of cyber threat detections in government networks and critical infrastructure each year.⁸ It was estimated that the number of detected cyber probes in 2024 alone exceeded 700 per minute.⁹ Although automated scans and minor intrusions are included in these numbers, they indicate a sustained and deliberate effort to chart vulnerabilities.

Breaches of major medical databases, such as high-profile attacks on leading health institutions in New Delhi, demonstrated the vulnerability of sensitive databases.¹⁰ Cybersecurity experts have also attributed some of the advanced campaigns to organizations with Chinese interests, including those in the energy, telecommunications, and health sectors. AI-enabled document forgery collides with espionage, where falsely obtained credentials are used to access restricted digital systems. A fake identity of a target employee, convincingly recreated on synthetic media, and approved authentication documents can be used to penetrate further than external attacks. The larger issue is that document forgery may serve as a gateway into secure conditions, and the line between cyber intrusion and identity fraud may be blurred. In a day and age when most people can access systems only through digital authentication rather than being physically present, infrastructure security cannot be separated from the integrity of documents.

- **Southeast Asian Transnational Scam Hubs:** In addition to actual geopolitical competition, India also faces transnational criminal bases in areas with weak governance. Organisations in some regions of Myanmar, Cambodia, and Laos have become the hubs of organised online fraud. People of different nationalities, including Indians, have been trafficked there under the pretext of being offered jobs, only to be coerced into performing massive scams on the internet.¹¹

These activities are based on data mining, AI-based voice cloning, and the generation of artificial documents. Fraudsters generate authentic identity credentials, law-enforcement notices, and banking documentation based on individual victims. The personalisation of the scam enhances the credibility and psychological pressure. The Indian government has been engaging in rescue and repatriation efforts, where thousands of its citizens who were forcibly lured into these activities have been taken back. But the structural forces of such hubs remain the same, supported by transnational financial flows and anonymity.

The introduction of these centres explains the interrelation of human trafficking, digital forgery, and financial crime. AI-generated document fabrication is not a single crime but a component of a network that exploits economic insecurity and the availability of technology.¹²

The Changing Legal and Regulatory Environment

India's legal response to cyber threats has developed gradually, but the rapid pace of technological advancement is straining the sufficiency of statutory laws.

- **Substantive IPC to BNS Law:** The implementation of a new Indian Penal Code, the Bharatiya Nyaya Sanhita, 2023, in place of the colonial-era Indian Penal Code, is a sign of an attempt to modernise substantive criminal law.¹³ New code makes direct reference to electronic records in its provisions on forgery, fraud, and document falsification. The legislature has sought to make people criminally liable in line with modern times by acknowledging digital records as part of the definition of public records. Stricter punishments for crimes against government documents reflect an understanding of the national security issue. But there are still complexities of doctrine. The concept of creating the mental aspect in cases of AI-generated content raises new questions. When a person uses an automated system to create falsified documents without hand modification, the intent attribution should also be carefully considered. Traditional methods of investigation also face the burden of proving the identity of the author of synthetic media.

The information Technology Act, 2000, has been of significant importance in the prosecution of identity theft and computer-related crimes.¹⁴ But its provisions were written before the spread of generative AI. Although passages on personation and data alteration can be modified, they do not specifically address synthetic media or algorithmic fabrication. The Unlawful Activities Prevention Act, 1967, will come into play when forgery of a document is used to promote terrorist activities, and its preventive detention policy should be exercised at all times with constitutional safeguards; it would otherwise be misused.¹⁵

- **Privacy and Data Protection:** The Digital Personal Data Protection Act, 2023, provides a legal framework for regulating the processing of personal data by non-governmental organizations and the state.¹⁶ The legal statute focuses on legal processing, limitation of purpose, minimisation of data, and accountability of data fiduciaries. Framed rules are more informative about obligations in situations where AI systems process biometric and image data. There are, however, exemptions to state functions concerning sovereignty, security, and the maintenance of order, which result in areas of tension. Although these exemptions are necessary to enforce the law, they should be strictly applied to avoid disproportionate infringement on individuals' privacy.

The legal system, as set out in *Justice K S Puttaswamy v Union of India*, is the guiding principle.¹⁷ Article 21 made the Supreme Court realise that privacy was inalienable to life and individual liberty. Any restriction should meet the standards of legality, legitimate aim, necessity, and proportionality. Within the framework of AI-driven forgery, this implies that data mining projects aimed at identifying fraudulent trends should be based on explicit statutory authority and supervised. Mass surveillance would not pass the proportionality test if it were indiscriminate.¹⁸

Defence and Countermeasures Nationally

India has been using a multi-layered strategy that combines technological innovation, regulatory reform, and inter-agency coordination to respond to AI-enabled threats. Border management systems are increasingly equipped with real-time surveillance cameras, motion sensors, and predictive analytics to detect suspicious mobility patterns. These systems aim to minimize reliance on strictly manual patrols and improve early detection of criminals.

Financial disruption strategies have become a priority for law enforcement agencies. Masses of SIM cards and device identifiers associated with unscrupulous activities have been prevented in a bid to shut down communication channels that perpetuate fraud.¹⁹ This has been made easier through coordination among banks and cybercrime cells to freeze suspicious bank accounts rapidly.

The Indian Computer Emergency Response Team holds regular mock downs that simulate ransomware and infrastructure attacks.²⁰ Such exercises engage hundreds of public and private bodies and are intended to assess readiness to counter a cyber-campaign. There has also been increased cooperation between countries.²¹ Bilateral information sharing and participation in international cybersecurity conferences and forums enable the exchange of information on new threats. Diplomacy has played a critical role in dealing with transnational scam centres and other operations to rescue victims of trafficking. Regardless of these attempts, the extent and flexibility of AI-enabled forgery require unceasing creativity.

Policy Recommendations

The AI-enabled document forgery policy proposal needs to balance security requirements with constitutional principles.²²

- Law enforcement agencies using investigative AI systems must be subject to transparency and audit provisions. Courts need to develop evidentiary principles that enable defence attorneys to assess the accuracy of algorithmic results. In the absence of this kind of protection, the likelihood of opaque decision-making is high.
- A comparison-driven model of regulation, inspired by the approach to AI regulations in the European Union, can be adjusted to Indian conditions. Applications that can create identity documents or alter biometric data must be treated as high-risk and meet strict compliance requirements.

- Efforts to create awareness among the people should be stepped up. The citizens are still the frontline against online fraud. Losses can be minimized by establishing clear channels of communication and timely reporting mechanisms to improve early detection.
- There should be judicial and prosecutorial capacity building. Further training on technical changes will enable more subtle adjudication of cases involving synthetic media or digital forgery.
- Oversight bodies should be strengthened to ensure that the expanded surveillance authority does not replace democratic accountability. Public trust can be enhanced through independent review boards and reporting.²³

Conclusion

The artificial intelligence-powered forgery of documents represents the sophistication of the modern national security problems. It does not exist in isolation as it overlaps with illegal migration, financing of terror, espionage, and transnational organised crime. The same technology that makes governance strong can also make deception strong.

The answer to India must then be multidimensional, including reforming the laws, innovating in technology, maintaining constitutional vigilance, and collaborating with other countries. The conflict between data mining and privacy cannot be resolved through trade-offs. Rather, it demands that proportionality, transparency, and accountability are the principles to follow.

The future of India's digital sovereignty will be determined by whether it is capable of securing identity systems without infringing on the rights that make its constitutional democracy. When dealing with AI-perpetrated forgery, the state should keep in mind that national security and personal freedom are not mutually exclusive but complementary sources of a stable republic.

References

1. National Crime Records Bureau, *Crime in India 2023: Statistics on Cyber Crimes* (Ministry of Home Affairs, Government of India, 2024).
2. Reserve Bank of India, *Annual Report 2024–25* (RBI, Mumbai, 2025).
3. Deloitte, *Trust in the Age of Generative AI: Deepfake Identity Fraud Report 2025* (Deloitte Global Security Survey, 2025).
4. World Economic Forum, *Global Cybersecurity Outlook 2026* (WEF, Geneva, 2026).
5. Unique Identification Authority of India, *Aadhaar Saturation and Digital Identity Statistics 2024* (UIDAI, Government of India, 2024).
6. Ministry of Home Affairs, *Border Management and Security Report 2025* (Government of India, 2025).
7. Financial Action Task Force, *Mutual Evaluation Report on Terror Financing Risks in South Asia* (FATF, Paris, 2024).
8. Indian Computer Emergency Response Team, *Cyber Security Threat Landscape Report 2024* (CERT-In, Ministry of Electronics and Information Technology, Government of India, 2024).
9. Ministry of Electronics and Information Technology, *Cyber Threat Monitoring Statistics 2024* (Government of India, 2024).
10. Press Information Bureau, Government of India, *Statement on Cybersecurity Incident Affecting AIIMS Delhi* (2023).
11. United Nations Office on Drugs and Crime, *Transnational Organized Crime in Southeast Asia: Cyber Scam Operations* (UNODC, Vienna, 2024).
12. Ministry of External Affairs, *Repatriation of Indian Nationals from Cyber Scam Compounds in Southeast Asia* (Government of India Press Release, 2025).
13. *Bharatiya Nyaya Sanhita, 2023*, No. 45 of 2023.
14. *Information Technology Act, 2000*, §§ 65, 66C, 66D.
15. *Unlawful Activities (Prevention) Act, 1967*, as amended in 2019.
16. *Digital Personal Data Protection Act, 2023*, No. 22 of 2023.

17. *Justice K.S. Puttaswamy v. Union of India*, (2017) 10 SCC 1.
18. Border Security Force, *Smart Border Surveillance and Integrated Security Systems Report 2025* (BSF Headquarters, Government of India, 2025).
19. Ministry of Home Affairs, *National Cyber Fraud Mitigation Strategy Report 2026* (Government of India, 2026).
20. Indian Computer Emergency Response Team, *Cyber Security Mock Drill Report 2025* (CERT-In, MeitY, Government of India, 2025).
21. INTERPOL, *Global Cybercrime Strategy 2024–2027* (INTERPOL, Lyon, 2024).
22. NITI Aayog, *Responsible AI for All: Strategy for India* (Government of India, 2023).
23. Ministry of Home Affairs, *National Cyber Crime Reporting Portal: Awareness and Citizen Reporting Statistics 2025* (Government of India, 2025).

