

AI-ENABLED SYNTHETIC IDENTITY FRAUD AND ONLINE VICTIMIZATION

***M. ASHWIN**

****R. VIMALA**

ABSTRACT

The swift emergence of generative Artificial Intelligence has further fueled the growth of AI-enabled synthetic identity fraud, wherein fraudsters leverage real, stolen, or fabricated personally identifiable information (PII) with deepfakes, voice clones, and AI-generated documents to build convincing fictitious personas. This complex cybercrime results in significant financial, psychological, and reputational damage to individuals and organizations, while threatening India's digital economy. This paper contends that India's current penal framework, largely governed by the Bharatiya Nyaya Sanhita (BNS), 2023, and the Information Technology Act, 2000, is ineffective in dealing with the distinctive challenges posed by AI-enabled synthetic identity, such as issues in determining mens rea, assigning liability, and affording adequate relief to victims of this complex cybercrime. The paper will examine the current legislative framework in dealing with identity-based cybercrimes, identify loopholes in existing laws, and suggest a new framework for dealing with this complex cybercrime, which poses a threat to India's digital economy. It critically analyzes the technological aspects of synthetic identity fraud, existing provisions in law (Sections 66C and 66D of the IT Act), issues in assigning liabilities, and the complex nature of victimization on the internet. The paper recommends legislative changes, which include insertion of a new chapter titled "Offenses Relating to Artificial Intelligence-Enabled Identity Fraud and Synthetic Personation" in the BNS or any other enactment as a separate law on AI Crimes. Recommendations include graded penalties with harsh punishments of 3-14 years' imprisonment, presumptive mens rea with a reverse burden of proof, corporate liability for not using AI-detection tools, victim compensation, National AI Fraud Victim Compensation Fund, and special fast-track courts.

*M. Ashwin, Student, School of Law, VISTAS

**R. Vimala, Assistant Professor, School of Law, VISTAS

The research highlights the critical need for these human rights-based legislative reforms to enhance deterrence, provide justice to victims, and align India's criminal justice system with the reality of the new generative AI technology landscape.

KEYWORD

Artificial Intelligence, Personally Identifiable Information, deepfakes, voice clones, mens rea,

INTRODUCTION

Synthetic identity fraud has quietly emerged as one of the financial crimes with the fastest rate of growth in recent years. The threat is now growing at an alarming rate due to the explosion of AI. Large-scale fraud can now be committed by fraudsters without the use of stolen identities. Instead, they can use AI-powered tools to create completely fictitious but incredibly convincing personas. For all businesses, this evolution raises an important question: Are conventional Know Your Customer (KYC) tools still useful?¹

One of the biggest threats you face today is the emergence of AI-powered synthetic identity fraud. **Deepfake and GenAI technologies** are being used more frequently to commit widespread fraud and get around conventional identity verification measures. The 2025 Datos Financial Crime and Cybersecurity Forum in Charlotte held an exceptional panel discussion titled "**Synthetic Identities 2.0: Detecting Fraud Enhanced With Deepfake Technology**" to address the problem and investigate ways to stay ahead of it. Experts from the financial services and cybersecurity industries participated in the discussion, including Eric Ondik, Senior Director of Market Development at **TransUnion®**.²

Cybercrime, or the use of computers or online networks for criminal purposes, includes everything from identity theft and fraud to intimidation and threats. Over the past 20 years, there has undoubtedly been an increase in cybercrime and its various forms. Every year, about 23% of households in the United States alone encounter some form of cybercrime.³

¹ Luke Boddie, Synthetic Identity Fraud In The Age Of GenAI: Are Traditional KYC Tools Still Fit For Purpose?, Forbes Business Development Council

² Transunion, Synthetic Identity Fraud 2.0: How AI Is Redefining Fraud Detection

³ James Hawdon, Cybercrime: Victimization, Perpetration, and Techniques, 2021 Nov 10;46(6):837–842

HYPOTHESIS

"The existing criminal law frameworks in India are inadequate to effectively address AI-enabled synthetic identity fraud and the resulting online victimization, and therefore require urgent reform through specific AI-fraud offences and victim-centric remedies."

STATEMENT OF THE PROBLEM

A sophisticated type of cybercrime known as AI-enabled synthetic identity fraud has emerged as a result of the quick development of generative AI. In this type of crime, criminals use deepfakes, voice cloning, and AI-generated documents to create and maintain fictitious or altered identities. This new scam puts people at risk of being victimised online, resulting in large financial losses, psychological distress, and reputational damage.

The **Information Technology Act, 2000** and the **Bharatiya Nyaya Sanhita** are the main pieces of the current criminal law framework, but they are insufficient to adequately address the particular difficulties presented by AI-driven synthetic identity fraud, despite the rising prevalence of such crimes in India. There are significant gaps in the definition of particular offences, the establishment of mens rea when AI tools are involved, the attribution of criminal liability in intricate AI-assisted schemes, and the provision of significant remedies to victims.

In addition to undermining the deterrent power of criminal law, this inadequacy deprives victims of online fraud of sufficient protection or compensation. Therefore, in order to improve India's criminal justice response in the era of generative AI, it is imperative to investigate these legal flaws and suggest targeted reforms, such as the introduction of specific AI-fraud offences and victim-centric mechanisms.

TECHNOLOGICAL DIMENSIONS OF AI-ENABLED SYNTHETIC IDENTITY FRAUD

By purposefully leaving a false digital footprint on social media and in public records, synthetic identities are created by fusing real and fake information to create a new persona. Bad actors then use these identities to carry out a variety of illegal activities, including fraud, misdirection,

and unauthorised access. **Synthetic identity fraud** creates completely new identities that may not be connected to a real person at all, even though some of the biographical or demographic information may be true, in contrast to traditional identity theft, which entails stealing an existing person's identity.

Fraudsters fabricate significant and historical details in order to make their synthetic IDs seem genuine and authentic. In order to make their false identities plausible and credible, thieves and bad actors, for example, use techniques known as "**Backstopping**" to create credible backstories that go far beyond simply using an SSN and credit history. They do this by combining real and fictional information to make their identities seem more convincing while also making them more difficult to spot. Synthetic IDs are being used more frequently and can be used in a variety of ways to defraud individuals and businesses. Although the precise amount lost to synthetic identity fraud is unknown, a Thomson Reuters report from 2023 put losses at "\$20 to 40 billion and growing."⁴

India is now a prime target for AI-driven scams due to its rapidly growing digital economy. With more than 800 million internet users in 2023, the nation is now the second-largest online market in the world, behind China (India Foundation, 2025). This, along with the rapid expansion of digital payments, has made it easier for cybercriminals to operate.⁵

INADEQUACIES OF EXISTING INDIAN CRIMINAL LAW FRAMEWORK

Cybercrimes have skyrocketed in tandem with India's swift digital transformation. The threat to people and organisations is real and includes everything from online banking fraud to the spread of offensive content and phoney social media accounts. The **Information Technology Act, 2000 (IT Act)** was introduced to address this. It has been modified over time to take into account more recent issues.

Four of its many provisions, **Sections 66C, 66D, 67, and 69A** stand out to regular internet users. Identity theft, online fraud, sharing pornographic material, and website blocking are all covered in these sections.

⁴ Moddy's "Synthetic identities and why they are important in today's digital landscape"

⁵ Safer Internet Lab's Research Report "Online Fraud and Scams in India" 2025

Section 66C: Identity Theft

This deals with cases where a person dishonestly uses another individual's identity information, such as a password, digital signature, or biometric data. This includes creating fake accounts on social media, stealing someone's credit card details, or impersonating them online. **The Punishment will be of Imprisonment up to 3 years and Fine up to ₹1 lakh**

Section 66D: Online Cheating and Impersonation

This section punishes cheating by impersonation using computer resources or communication devices. In simpler terms, if someone pretends to be another person online to deceive others for monetary or personal gain, this section applies. **The Punishment be of Imprisonment up to 3 years and Fine up to ₹1 lakh**

Section 67: Publishing Obscene Material Online

This section makes it illegal to publish, transmit, or share obscene or sexually explicit content on the internet. This includes images, videos, or any digital content that is considered obscene under Indian law. **The Punishment be of up to 3 years imprisonment + fine up to ₹5 lakh; Subsequent conviction of up to 5 years imprisonment + fine up to ₹10 lakh**

Section 69A: Power to Block Websites

This section gives the Government of India the power to block public access to information through any computer resource. This usually applies to websites or online platforms that pose threats to national security, public order, or morality. **The Punishment will be up to 7 years imprisonment + Possible fines⁶**

Dealing with criminal responsibility when AI systems cause harm is really tough for the usual legal setups we have. In Indian criminal law, things like ***mens rea*, the mental part, and *actus reus***, the action part, just do not fit well with how algorithms work. AI does not have thoughts or feelings like people do, or clear physical moves that you can pin blame on. It seems like the **Bharatiya Nyaya Sanhita from 2023**, along with other laws in India, leaves some big holes in holding AI accountable.

⁶ Laws Study "Cyber Laws in India: Understanding IT Act Sections 66C, 66D, 67 & 69A" Aug 2025

This gets messy when you try to apply those rules to machines making decisions. I am not totally sure, but it feels like the law assumes everything is human centered, which AI clearly is not. The provisions in the Sanhita talk about intent and acts, but they break down with code and data running things.⁷

CHALLENGES IN LIABILITY ATTRIBUTION AND PROSECUTION

Determining the criminal liability of AI in the context of the law in India is beset with a plethora of complex challenges, which converge at the crossroads of technology and law. As the technology of AI is increasingly being employed in society, the question of criminal liability for the criminal acts perpetrated through the medium of AI technology is increasingly becoming important in the legal arena. One of the challenges is the independence of the **AI algorithm**, which functions without any human intervention. Unlike humans, the AI algorithm does not possess any conscience and moral judgment. It is not possible to establish the mens rea or guilty mind in the context of the criminal liability of the AI algorithm. The lack of legal personhood for AI systems also creates further complexities. In India, as well as in many countries, the legal personhood is granted to human beings as well as some entities such as corporations but not to AI systems. Therefore, the lack of legal personhood for AI means that the AI system cannot be regarded as an entity with the right to do certain things, including the commission of criminal acts. The issue that arises is who the responsibility lies with when the AI system is involved in the commission of criminal acts, whether the developer, the user, or the operator of the AI system is held liable.

The issue of criminal responsibility for AI becomes more pertinent in scenarios involving the application of AI in areas involving higher stakes, like autonomous vehicles or medical diagnostic systems. For example, in the event of an accident caused by an AI-based autonomous vehicle, resulting in loss of life, should the manufacturer of the AI or the owner of the vehicle be held criminally liable? The determination of responsibility becomes more important in scenarios involving AI, which can have life-altering effects. Additionally, the rise

⁷ Akanksha Priya's Lawfoyer International Journal of Doctrinal legal Research "CRIMINAL ACCOUNTABILITY FOR AI: MENS REA, ACTUS REUS, AND THE CHALLENGES OF AUTONOMOUS SYSTEMS" ISSN: 2583-7753

of AI-based fake content, like deepfakes, poses another challenge to the legal systems of the world, including India.⁸

NATURE AND IMPACT OF ONLINE VICTIMIZATION

The use of AI in synthetic identity theft consists of the creation of new fictitious identities through the combination of legitimate, stolen, or fictitious personally identifiable information (PII), such as **social security numbers, names, addresses, and other AI-generated documents, images, or deepfakes**. The use of generative AI in synthetic identity theft speeds up the creation of new fictitious identities by rapidly producing legitimate-looking supporting documentation, such as **fictitious identification documents, credit reports, or images**, making it much more difficult to detect compared to other forms of identity theft.

The impact of this type of fraud is specific, yet related, to several aspects: financial, psychological, and reputational. Although synthetic identity theft does not have a "**real**" victim in the context of its creation, it often employs legitimate PII, such as that of minors, deceased persons, or data breach victims.

1. Financial Harm

Monetary loss is the biggest consequence of AI-based synthetic identity fraud. It involves huge direct and indirect monetary loss to individuals, financial institutions, businesses, and the economy. Perpetrators "age" the synthetic identities to establish credit histories with small legitimate-looking transactions, followed by large-scale fraud, including loan defaults, credit card fraud, and money laundering. It is being fueled by the advent of generative AI, which is being used to develop corroborating documents such as pay stubs, utility bills, and deepfake images.⁹

According to estimates, synthetic identity theft resulted in a loss of about \$35 billion in 2023, and this figure is likely to increase sharply in the coming years due to the use of AI technology. Moreover, Deloitte has forecasted that tens of billions of dollars more will be lost by 2030. Financial institutions incur significant unrecoverable costs due to

⁸ Taylor and Francis online, "Artificial intelligence and criminal liability in India: exploring legal implications and challenges", Law, Criminology and Criminal Justice, Article: 2343195, Apr 2024

⁹ The Federal Reserve, "GENERATIVE ARTIFICIAL INTELLIGENCE INCREASES SYNTHETIC IDENTITY FRAUD THREATS"

fraudulent accounts, overdrafts, and refunds. On the other hand, victims incur significant personal costs such as credit scores, time, and money. The elderly population is also more affected by identity theft, with a loss of about \$200 to \$1,453 per case, but the total impact can run into the billions of dollars, such as the loss of about \$2.5 billion for the elderly population in 2016, before the use of AI technology for such crimes.¹⁰ Moreover, the use of AI technology in social engineering, such as deepfake impersonation, will increase the losses due to authorized push payment scams or account takeover fraud.¹¹

2. Psychological Harm

The emotional toll on victims of synthetic identity theft carried out through the use of artificial intelligence technology is considerable, often on par with or even more so than traditional identity theft due to the prolonged nature of these crimes. Even though the identity theft itself is on a synthetic identity, there is emotional distress for those whose personal information is being used for these crimes or who fall victim to these scams. Empirical research on identity theft victimization has shown moderate to severe emotional distress in about one-third of cases, including anxiety, stress, depression, anger, shame, and embarrassment. The aggravating effects of victimization include time spent resolving the incident (positively correlated with emotional distress), financial losses including credit problems, and interpersonal difficulties. Females and minorities, as well as older adults, experience more emotional distress as a result of victimization. AI contributes to emotional distress by hyper-personalizing social engineering tactics, including **deep fake and voice cloning technology**, which can lead to a lack of trust in personal communication and a sense of being vulnerable.¹²

The psychological weaknesses exploited by AI fraudsters, such as curiosity, helpfulness, or the pressure of urgency in phishing schemes, result in secondary trauma from coerced transactions or extortion. In legal analyses, the technical and human aspects involved in AI manipulation are said to create “an illusion that feels deeply personal, leaving psychological scarring.”¹³

¹⁰ Steven M Albert, “The Financial and Psychological Impact of Identity Theft Among Older Adults”, National Library of Medicine, PMCID: PMC8699092 PMID: 34988295

¹¹ AI-driven financial fraud: key risks and legal protections for financial institutions, Journal of Banking Regulation, Volume 27, article number 6, (2026)

¹² Supra, at 11

¹³ Supra, at 12

3. Reputational Harm

The consequences of reputational losses arising from AI-based synthetic identity fraud include those experienced by financial institutions as well as businesses. In the case of financial institutions as well as businesses, the consequences of high-profile synthetic identity fraud include media attention, customer complaints going viral, regulatory actions, as well as losses in terms of customer confidence.¹⁴

Synthetic fraud's "unseen" aspect means that the lack of an immediate real victim to complain about the issue delays the discovery but increases the impact when the issue is discovered, such as negative reviews, press coverage of the breaches, or regulatory actions against the institution. The role of AI in the construction of hyper-realistic identities increases the impact as more extensive schemes are possible, gaining the attention of the public.¹⁵

For the individual, the misuse of PII in synthetic fraud schemes results in credit score degradation, denied loans/services, or employment issues, which negatively reflects on personal reputation. Strained relationships with family due to issues related to the identities further contribute to the negative reputation.¹⁶

In the context of criminal law in India, there is no direct law applicable to the commission of crimes involving the use of AI-based tools for the creation of synthetic identities and deepfake impersonation. Instead, these crimes fall under the broad category of cheating by personation (**BNS sec 318, equivalent to the IPC sec 419**), forgery (**BNS sec 336 and 337**), the **Information Technology Act sec 66C (identity theft) and sec 66D (cheating by personation using computer resources)**. These provisions were established prior to the advent and popularization of generative technology and, as such, are not applicable to the "non-existent" criminals generated by the aforementioned tools.¹⁷

Cyberlaw specialist Pavan Duggal states, **"Today, these offences are loosely fitted into provisions on cheating or forgery. It is high time the law is re-examined. Until then, these crimes will continue with no recourse."**

¹⁴ Supra, at 12

¹⁵ Christopher Tennyson, "Synthetic Identity Fraud: The Unseen Threat and Its Cost to Businesses", Identity & Fraud, Equifax Insights Blog, Dec 2025

¹⁶ Supra, at 11

¹⁷ Vitasta Kaul, Reason under arrest "How digital arrest scams exploit fear to psychologically manipulate their victims into parting with money", Feb 2026

In the aforementioned context, it is evident that the victim is being duped by the AI tools, such as deepfake videos and voice clones used in digital arrests.¹⁸

REFORM PROPOSALS FOR INDIAN CRIMINAL LAW

The emergence of several generative tools of AI technology has elevated synthetic identity fraud to a new level of sophistication and scalability in India. Scammers are using real, stolen, and even fake **personally identifiable information (PII)**, combined with deepfakes, voice clones, and fake documents created by AI technology, to establish nonexistent ‘identities’ that evade Know Your Customer requirements, establish credit histories, and perpetrate massive financial crimes. The existing provisions of the **Bharatiya Nyaya Sanhita, 2023 (BNS), Information Technology Act, 2000 (IT Act), and amendments of 2025-2026 to the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules** are primarily geared towards intermediary liability and general cheating and identity theft. The existing provisions are not sufficient to create specific offenses for the nuances of AI-enabled synthetic identity fraud.

The current criminal law regime in India is based on general offenses such as **cheating by personation (BNS Sec 318, formerly IPC Sec 419), forgery of electronic records (BNS Sec 336 to Sec 337), identity theft (IT Act Sec 66C), and cheating by personation using computer resources (IT Act Sec 66D)**. These provisions are based on the assumption of human actors and traditional means of deception. They do not take into account the following hypothetical situations:

- No single “real” wrongdoer is present during the creation of the account, as the AI creates corroborating documents, biometric data, and transaction history.
- Synthetic identities may be “aged” over time before the commission of the major fraud.
- Hyper-realistic social engineering enabled by deepfakes and voice clones challenges the distinction between technology-based deception and human deception.¹⁹

¹⁸ Sakshi Soni, “DEEPFAKE AND AI CRIMES IN INDIA: THE URGENT NEED FOR A STRONG LEGAL FRAMEWORK”

¹⁹ Aayushman Verma, Manik Tindwani “Accountability By Design: Shared Liability In AI Fraud Under Indian Cyber Law”, Virtuosity legal, Sept 2025

The 2025-2026 **IT Rules**’ amendments propose a new term **“Synthetically Generated Information” (SGI)** and require labeling, removal of content in 2-3 hours in cases of high risk, e.g., impersonation, forged documents, and taking various forms of technology action by intermediaries. These are regulatory due diligence requirements on intermediaries and not criminal provisions under the BNS. They do not create direct liability on creators/distributors of AI systems used in financial fraud schemes. Sanctions continue to depend on general provisions of the IT Act (up to 3 years’ imprisonment and fines) and are insufficient in cases of multi-crore rupee losses and systemic risk to financial stability.²⁰

Legal experts emphasize how generic provisions can cause difficulties in prosecution due to difficulties in establishing evidence and proving “mens rea” in cases of AI systems’ semi-autonomous actions and unintended consequences of a foreseeable nature.²¹

RECOMMENDATION AND WAY FORWARD

1. Legislative Reforms: Introduction of Specific AI-Fraud Offences

A new standalone chapter should be included in the BNS under a new title: **“Offences Relating to Artificial Intelligence-Enabled Identity Fraud and Synthetic Personation”** (which can be enacted as a separate AI Crimes Act). It should include “Synthetic identity” as any persona created by combining real, stolen, or fictitious personally identifiable information (PII) with AI-generated content such as deepfakes, voice clones, forged documents, or fabricated transaction histories.

2. Institutional and Enforcement Mechanisms

To Establish dedicated units in the **Central Bureau of Investigation (CBI)** and **police forces across states (under the aegis of the Indian Cyber Crime Coordination Centre— I4C)**, which shall have experts in digital forensics, AI ethics, and financial investigation. These units shall be provided with mandatory deepfake detection and

²⁰ Freshfields, “India targets deepfakes and AI-generated content: key changes under MeitY’s 2026 amendments to the IT Rules”, Feb 2026

²¹ Niharika Jorwal, “Deepfake Technology and Criminal Law Reform in India: Addressing Synthetic Media Under the Bharatiya Nyaya Sanhita, 2023”, International Journal For Multidisciplinary Research, E-ISSN: 2582-2160

synthetic identity forensics toolkits. Mandatory training programs to be conducted annually for judicial, prosecution, and investigation authorities regarding AI forensics, chain of custody in generative models, and attributing liability in multi-actor AI systems.

3. Technological and Regulatory Safeguards

All generative-AI tools being made available in India should be required to carry invisible, tamper-proof watermarks and metadata. Intermediaries should be required to reject unlabelled synthetic content in financial onboarding processes.

Consider implementing a tiered model, with high-risk AI applications such as financial KYC, credit scoring, and deepfake generation being subject to conformity assessments, human oversight, and audits.

CONCLUSION

The hypothesis that existing criminal law regimes in India are insufficient to deal with AI-enabled synthetic identity frauds and victimization on the internet has stood the test of truth. From the analysis, it is evident that the existing Bharatiya Nyaya Sanhita, 2023, and Information Technology Act, 2000, are incapable of dealing with the new challenges posed by generative AI, such as synthetic identity, deepfakes, mens rea, and victimization on the internet. Such a situation is detrimental to the interests of citizens, who are exposed to serious financial, psychological, and reputational risks on the internet. Therefore, there is a need for legislative reforms in this area, which will help in deterring such crimes and providing justice to victims of AI-enabled frauds on the internet. India needs to take immediate steps to align its criminal justice system with the reality of the generative AI phenomenon, which will help in protecting its citizens while promoting responsible innovation in this field.

REFERENCE

<https://www.forbes.com/councils/forbesbusinessdevelopmentcouncil/2025/07/14/synthetic-identity-fraud-in-the-age-of-genai-are-traditional-kyc-tools-still-fit-for-purpose/>

<https://www.transunion.com/blog/detecting-synthetic-identity-fraud-enhanced-by-ai>

<https://pmc.ncbi.nlm.nih.gov/articles/PMC8579169/>

<https://www.moodyys.com/web/en/us/kyc/resources/insights/synthetic-identities-and-why-they-are-important-in-todays-digital-landscape.html>

https://saferinternetlab.org/wp-content/uploads/2025/06/Research-Report-A4_Fraud-India.pdf

<https://lawsstudy.com/cyber-laws/>

<https://www.tandfonline.com/doi/full/10.1080/23311886.2024.2343195#abstract>

<https://fedpaymentsimprovement.org/wp-content/uploads/sif-toolkit-genai.pdf>

<https://pmc.ncbi.nlm.nih.gov/articles/PMC8699092/>

<https://link.springer.com/article/10.1057/s41261-025-00304-y>

<https://pmc.ncbi.nlm.nih.gov/articles/PMC8699092/>

<https://frontline.thehindu.com/social-issues/ai-deepfake-digital-arrest-scams-india-cybercrime/article70587955.ece>

<https://www.jusscriptumlaw.com/post/deepfake-and-ai-crimes-in-india-the-urgent-need-for-a-strong-legal-framework>

<https://virtuositylegal.com/accountability-by-design-shared-liability-in-ai-fraud-under-indian-cyber-law/>

<https://technologyquotient.freshfields.com/post/102mjwn/india-targets-deepfakes-and-ai-generated-content-key-changes-under-meitys-2026>

<https://www.ijfmr.com/research-paper.php?id=71885>