INTERNATIONAL JOURNAL OF HUMAN RIGHTS LAW REVIEW
An International Open Access Double Blind Peer Reviewed, Referred Journal

Volume 5 | Issue 1 | 2026 Art. 05

A Study on Identity Theft in Relation to Digital Personal Data Protection Act, 2023

Adithya Yegan
Law Student, 1st Year, LL.M.,
Crime & Forensic Law, School of Excellence in Law,
The Tami Nadu Dr. Ambedkar Law University, Chennai

T. Vaishali
B.A., B.L (Hons.), L.L.M., Ph.D. (pursuing),
Assistant Professor of Law, Department of Criminal Law and Criminal Justice Administration, Tamil Nadu Dr. Ambedkar Law University, Chennai

Recommended Citation
Adithya Yegan and T. Vaishali, *A Study on Identity Theft in Relation to Digital Personal Data Protection Act, 2023*, 5 IJHRLR 70-85 (2025).
Available at www.humanrightlawreview.in/archives/.

A Study on Identity Theft in Relation to Digital Personal Data Protection Act, 2023

Adithya Yegan
Law Student, 1st Year, LL.M.,
Crime & Forensic Law, School of Excellence in Law,
The Tami Nnadu Dr. Ambedkar Law University, Chennai

T. Vaishali
B.A., B.L (Hons.), L.L.M., Ph.D. (pursuing),
Assistant Professor of Law, Department of Criminal Law and Criminal Justice Administration, Tamil Nadu Dr. Ambedkar Law University, Chennai

Manuscript Received	Manuscript Accepted	Manuscript Published
28 Dec. 2025	30 Dec. 2025	06 Jan. 2026

ABSTRACT

This paper explores the socio-legal ecosystem of identity theft in India, tracing the evolution of the threat landscape, the limitations of previous legal regimes, and the structural promises of the new legislative framework. The major objectives of the study are to assess the legal framework's agility in addressing emerging threats like Synthetic Identity Theft and AI-driven deepfakes, to formulate evidence-based recommendations for the Data Protection Board to strengthen the enforcement regime and to examine the effectiveness of the existing legislations, tool & techniques that safe guard Identity Theft. While amending the Act is a legislative hurdle, the government can leverage the Consumer Protection Act, 2019 in tandem with DPDP. Currently, the DPB handles data compliance, and the Police handle identity theft (BNS). There is an operational silo. A formal information-sharing protocol should be established between the Data Protection Board and the Indian Cyber Crime Coordination Centre (I4C). The Digital Personal Data Protection Act, 2023, marks a decisive, albeit imperfect, step towards maturing India's digital economy. By imposing high-cost penalties on negligence, it seeks to dry up the supply of stolen data that fuels the identity theft industry. Section 8's security mandates and Section 33's punitive caps effectively serve as a high wall against mass data breaches, forcing corporate India to internalize the cost of cybersecurity.

KEYWORDS

Identity, Cyber Security, Data, Artificial Intelligence & Technology.

1. INTRODUCTION

The enactment of the Digital Personal Data Protection Act, 2023 (DPDP Act) and the subsequent notification of the Digital Personal Data Protection Rules, 2025 mark the most significant overhaul of India's informational privacy landscape in the 21st century. As the nation transitions into a fully digitized economy, the protection of personal identity has ceased to be merely a matter of civil liberty; it has become a critical component of national security and economic stability. This introduction explores the socio-legal ecosystem of identity theft in India, tracing the evolution of the threat landscape, the limitations of previous legal regimes, and the structural promises of the new legislative framework.

1.1 The Digital Transformation and Expanded Threat Surface

The trajectory of India's digital evolution has been nothing short of exponential. Under the Digital India initiative, the nation has integrated over a billion citizens into a unified digital infrastructure. Recent government data reveals that over 86% of Indian households are now connected to the internet, creating a massive, interconnected population that relies on digital platforms for banking, healthcare, governance, and social interaction.[1] This rapid digitization, while democratizing access to services, has inadvertently expanded the attack surface for cybercriminals.

The statistics paint a grim picture of this vulnerability. Cybersecurity incidents in India have more than doubled in a span of two years, escalating from 10.29 lakh in 2022 to over 22.68 lakh in 2024.[1] This surge is not merely a function of increased users but reflects a qualitative shift in the nature of crime. Identity theft has moved from physical theft of documents to sophisticated, automated data extraction. In the financial sector alone, Account Takeover (ATO) fraud—where a criminal uses stolen identity credentials to hijack a user's bank account—now accounts for 55% of all fraud cases in India.[2] The scale of the crisis is further evidenced by the Union Budget 2025-2026, which felt compelled to allocate ₹782 crore specifically for cybersecurity projects to stem this tide, acknowledging that the digital trust of

[1] Curbing Cyber Frauds in Digital India, 2025
[2] BioCatch Releases 2024 Digital Banking Fraud Trends in India, 2024

the citizenry is under siege.

1.2 The Epidemiology of Modern Identity Theft

To understand the relevance of the DPDP Act, one must first categorize the pathology of identity theft it aims to curb. In the contemporary Indian context, identity theft has metastasized into three distinct but overlapping categories:

- **Financial Identity Theft:** This remains the most prevalent form, driven by the immediate monetization of stolen data. Cybercriminals utilize stolen Aadhaar numbers, PAN details, and biometric data to open fraudulent bank accounts or secure unauthorized loans. A recent report highlights a disturbing trend of mule accounts, where a single device is often used to log into an average of 35 different bank accounts, indicating highly organized syndicates operating fraud factories in regions often referred to as Jamtara clusters.[2]

- **Synthetic Identity Fraud:** A more insidious evolution is synthetic identity theft, where criminals do not steal a single person's entire identity but combine real information like a stolen Aadhaar number with fake information such as an AI-generated face or a fake address to create a new, non-existent identity. This Frankenstein identity is then used to build a credit score and eventually defraud financial institutions. Reports indicate that synthetic identity fraud is becoming the fastest-growing financial crime, as traditional verification systems struggle to flag identities that are partially real.

- **The Deepfake Frontier:** The year 2024-2025 has witnessed the weaponization of Artificial Intelligence in identity crimes. Deepfake technology allows criminals to clone voices and faces, bypassing video KYC (Know Your Customer) norms and biometric security. Global reports suggest that deepfake fraud attempts occurred every five minutes in 2024, with a staggering 3,000% increase in deepfake volumes between 2022 and 2023. This technological leap renders traditional definitions of data theft obsolete, as the threat is no longer just about stealing data, but simulating it.

1.3 The Legislative Vacuum: The Failure of the IT Act, 2000

For over two decades, India’s defense against this onslaught was the Information Technology Act, 2000. While pioneering for its time, the IT Act struggled to keep pace with the velocity of modern data processing.

- **The Compensation Model (Section 43A):** The primary remedy for identity theft victims lay in Section 43A of the IT Act. This provision mandated that if a body corporate was negligent in implementing reasonable security practices, it was liable to pay damages directly to the affected individual. While this seemingly favoured the victim, in practice, it was ineffective. The adjudication process was slow, the burden of proof on the victim was high, and the reasonable security practices were often interpreted loosely.

- **The Privacy Jurisprudence:** The legal landscape shifted seismically with the Supreme Court's judgment in Justice K.S. Puttaswamy v. Union of India (2017). The Court declared privacy a fundamental right under Article 21 of the Constitution. This judgment necessitated a dedicated data protection law that went beyond the compensation model of the IT Act and established a rights-based framework for data processing. The Court argued that the state has a positive obligation to protect the informational privacy of its citizens, leading directly to the drafting of the DPDP Act.[3]

1.4 The DPDP Act, 2023: A Structural Paradigm Shift

The Digital Personal Data Protection Act, 2023 represents a fundamental departure from the tort-based approach of the IT Act to a compliance-based regulatory regime. It operationalizes the balance between individual rights and lawful processing needs.

- **From Compensation to Penalty:** The most controversial aspect of this transition is the repeal of Section 43A of the IT Act. The DPDP Act focuses on penalizing the Data Fiduciary the entity processing data rather than compensating the Data Principal. Under Section 33, the Data Protection Board of India (DPBI) can impose penalties of up to ₹250 crore for security failures. However, these penalties are credited to the Consolidated Fund of India, not the victim. This shifts the law's focus from restituting individual loss to deterring corporate negligence.[4]

- **The Digital Scope:** Unlike the GDPR, which covers all personal data, the DPDP Act applies specifically to digital personal data collected online or offline data that is subsequently digitized. This distinction is crucial in a country where vast amounts of identity data like physical photocopies of Aadhaar cards still circulate in non-digital forms,

[3] India's Digital Personal Data Protection Act 2023: A Landmark in Data Protection, 2023
[4] Penalties by board -Digital Personal Data Protection Act, 2023 DPDPA Sec. 33 interpretation, 2024

potentially falling outside the Act's immediate purview until digitized.

1.5 The Intersection with Criminal Law: Bharatiya Nyaya Sanhita (BNS)

While the DPDP Act handles the regulatory aspect of data handling, the criminal act of identity theft is now governed by the Bharatiya Nyaya Sanhita, 2023 (BNS), which repealed the Indian Penal Code (IPC) 1860. The interface between these two laws is critical for understanding identity theft prosecution.

- **Cheating by Personation (Section 319 BNS):** Replacing Section 416 of the IPC, this section criminalizes the act of pretending to be another person. Crucially, the BNS explanation clarifies that the offence is committed whether the individual personated is a real or imaginary person, thereby providing a legal hook to prosecute synthetic identity theft.

- **Forgery of Electronic Records (Section 336 BNS):** This section addresses the creation of false electronic records with intent to cause damage or injury. In the context of the DPDP Act, if a Data Fiduciary's negligence facilitates a breach, the Fiduciary faces a civil penalty under the DPDP Act, while the hacker faces criminal prosecution under Section 336 of the BNS.

- **Organized Crime (Section 111 BNS):** Recognizing that identity theft is often a syndicated activity, the BNS introduces specific provisions for organized crime, allowing for stricter bail and sentencing for gangs operating identity theft rings.[5]

Objectives of the Study

- To assess the legal framework's agility in addressing emerging threats like Synthetic Identity Theft and AI-driven deepfakes.

- To formulate evidence-based recommendations for the Data Protection Board to strengthen the enforcement regime.

- To examine the effectiveness of the existing legislations, tool & techniques that safe gaurd Identity Theft.

2. REVIEW OF LITERATURE

[5] India Antivirus Market Analysis, Size, and Forecast 2025-2029 – Technavio, 2025

(Anderson 2008) Identity theft is made possible by the nature of modern payment systems. In the modern economy, sellers are willing to offer goods and services to strangers in exchange for a promise to pay, provided the promise is backed up by data that link the buyer to a specific account or credit history. Identity theft involves acquiring enough data about another person to counterfeit this link, enabling the thief to acquire goods while attributing the charge to another person's account. In this article, we discuss what is (and is not) known about the prevalence and cost of identity theft, describe the institutional framework in which identity theft takes place, and consider some of the main policy issues associated with the problem.

(Vijaya Geetha 2011) Today almost all businesses are connected online and net banking has becoming a buzzword. The concept of identity theft which was more known in the Western world is making its presence felt in developing economies like India. A few statistics related to the phishing attacks worldwide are compared with India's to gauge the severity of the problem. There has been an increase in identity theft in the last few years which could pose a serious problem in the future, resulting in loss of trust by the customer towards net banking. Most of the Indian banks are taking initiatives to address the problem but still more work is to be done in the case of small and rural banks.

(Bradford W Reyns & Billy Henson 2015) Available evidence suggests that identity theft is a growing problem that has significant consequences for victims, not the least of which is billions of dollars in financial losses. However, very little is known about the correlates or causes of identity theft victimization. Utilizing a nationally representative sample of individuals from the Canadian General Social Survey, the current study attempts to address this deficiency by examining the link between victims' online routine activities and their online identity theft victimization. It was found that certain routine activities directly influence the likelihood of experiencing identity theft. Potential research and policy implications also are discussed.

(F Cassim 2015) The increased use of the Internet for business and financial transactions, social networking and the storage of personal information has facilitated the work of identity thieves. Identity theft has an impact on the personal finances and emotional well-being of victims, and on the financial institutions and economies of countries. The article examines measures introduced by the respective governments in these countries to counteract such crimes. It is advocated that businesses and institutions should take measures to protect personal information better and that individuals should be educated about their rights, and be vigilant and protect their personal information offline and

in cyberspace.

(Mehdi Dadkhah 2017) In recent years, identity theft has been growing in the academic world. Cybercriminals create fake profiles for prominent scientists in attempts to manipulate the review and publishing process. Without permission, some fraudulent journals use the names of standout researchers on their editorial boards in the effort to look legitimate. This opinion piece, highlights some of the usual types of identity theft and their role in spreading junk science. Some general guidelines that editors and researchers can use against such attacks are presented.

(Kiran Saini 2021) This paper explores the legal and behavioral aspects of privacy and identity theft across multiple contexts, drawing on leading studies and legal analyses from the United States and India. Highlights gaps in protection and enforcement. Behavioral studies on privacy paradoxes, smartphone data risks and identity theft are integrated to provide a nuanced understanding of user behavior and systemic vulnerabilities. By synthesizing interdisciplinary perspectives—legal, technological and behavioral—the paper argues for stronger legal frameworks, public awareness and ethical technology design to protect privacy in an era of pervasive surveillance and data exploitation.

(Langton 2021) In this paper, the author addresses identity theft's prevalence and cost, outlines the institutional setting in which it occurs, and takes into account some of the key policy concerns related to the issue. Modern payment systems' inherent vulnerabilities make identity theft possible. As long as the promise of payment is supported by information that links the user to a specific account or credit history, vendors are prepared to provide products and services to strangers in the contemporary economy.

(Carla Sofia Cardoso 2022) The present study aims at understanding what factors contribute to the explanation of online identity theft (OIT) victimization and fear, using the Routine Activity Theory (RAT). Additionally, it tries to uncover the influence of factors such as sociodemographic variables, offline fear of crime, and computer perception skills. Data for the present study were collected from a self-reported online survey administered to a sample of university students and staff. Fear of OIT was explained by socioeconomic status, education and by fear of crime in general.

(Dr. Rahul Kailas Bharati 2025) The digital era, an individual's identity is increasingly represented and verified through electronic means. Unique identifiers such as passwords, electronic signatures, biometric data, and other personal authentication details serve as keys to our digital lives, granting access to bank

accounts, social media profiles, email communications, and a plethora of online services. The chapter will explore the requisite mens rea for conviction, examine the prescribed punishments, and differentiate between these two critical sections. Through a rich tapestry of examples, real-life scenarios, practical case studies, and relevant Indian judicial pronouncements, we aim to equip readers with a thorough understanding of how these provisions are interpreted and applied. Furthermore, we will discuss the interplay of these sections with other relevant laws, such as the Bharatiya Nyaya Sanhita (BNS), 2023 (formerly the Indian Penal Code, 1860), and the challenges encountered in the investigation and prosecution of these insidious cybercrimes.

(Md Moeen Ajaz Khan 2025) Identity theft in India is an urgent concern due to increasing digitalization, widespread use of government-issued identification, and evolving cybercrime tactics. The study explores the complex interactions between individual privacy, institutional protections, and social vulnerability, highlighting how misuse of Aadhaar, PAN, and banking infrastructure enables largescale financial fraud. The research contextualizes contemporary legal safeguards, scrutinizes judicial responses, and identifies systemic failures using statutory, empirical, and case-based evidence. Ultimately, the paper advances comprehensive policy and technological recommendations to reinforce protections, mitigate harm, and balance public utility against personal privacy rights.

(Pablo Madriaza 2025) People use social media platforms to chat, search, and share information, express their opinions, and connect with others. The objective of this review is to synthesize the empirical evidence on how media exposure to hate affects or is associated with various outcomes for individuals and groups. Fifty-five studies analyzing 101 effect sizes, classified into 43 different outcomes, were identified after the screening process. This systematic review confirms that exposure to hate in online and in traditional media has a significant negative impact on individuals and groups. It emphasizes the importance of taking these findings into account for policymaking, prevention, and intervention strategies. Hate speech spreads through biased commentary and perceptions, normalizing prejudice and causing harm.

3. THE EVOLUTION FROM PRIVACY TO DATA PROTECTION

Legal scholars have long argued that the Information Technology Act, 2000 was structurally ill-equipped to handle the complexities of modern data processing. The seminal Supreme Court judgment

in Justice K.S. Puttaswamy v. Union of India (2017)[6], which recognized privacy as a fundamental right under Article 21, necessitated a standalone data protection law. Notably, the 2018 draft explicitly defined identity theft as a specific harm, whereas the 2023 Act removed the definition of harm entirely, relying instead on the Data Protection Board's discretion in assessing penalties. This omission is critical, as it removes the explicit statutory recognition of identity theft as a distinct injury resulting from data processing failures.

3.1 The Compensation Vacuum Debate

A dominant theme in contemporary legal commentary is the Compensation Void. Under the previous regime (Section 43A of the IT Act), if a body corporate was negligent in maintaining reasonable security practices, it was liable to pay damages directly to the affected individual. The DPDP Act repeals this section. Critics argue this creates a perverse incentive where the state benefits financially from data breaches via penalties, while the victim who suffers the actual trauma of identity theft is left to pursue lengthy civil suits or common law remedies with no statutory guarantee of compensation. The Internet Freedom Foundation (IFF) has consistently flagged this as a regression in citizen rights, noting that victims of massive breaches—like the ICMR Aadhaar leak affecting 81.5 crore Indians—are left without a streamlined compensation mechanism under the new law, effectively prioritizing corporate stability over individual restitution.

3.2 Security Safeguards: The Reasonable Standard

The literature also focuses heavily on the definition of reasonable security safeguards under Section 8(5) of the DPDP Act. Comparative studies with the European Union's GDPR note that while GDPR mandates appropriate technical and organizational measures based on risk assessments, the DPDP Act uses the term reasonable, a standard that is often litigated and subjective. However, the notification of the 2025 Rules is expected to standardize these measures, bringing India closer to global norms like ISO 27001, though the effectiveness of enforcement by the Data Protection Board (DPB) remains a subject of prospective analysis.[7]

3.3 The Threat Landscape: From Credit Cards to Synthetic Identities

[6] AIR 2018 SC (SUPP)
[7] Decrypting India’s Data Protection Regime: The Data Protection Board of India, 2025

Cybersecurity literature provides the empirical basis for understanding the urgency of the DPDP Act. The Identity Theft Resource Center (ITRC) 2024 report highlights that identity theft is no longer limited to stealing credit card numbers but has evolved into Synthetic Identity Fraud combining real and fake data to create new identities that are harder to detect.

4. STATISTICAL OVERVIEW OF THE CRISIS

The digital explosion in India has been accompanied by a corresponding explosion in cyber fraud, creating a crisis of confidence in digital platforms[8].

- **Incident Volume:** According to government data, cybersecurity incidents in India escalated from 10.29 lakh in 2022 to over 22.68 lakh in 2024. This doubling of incidents in a mere two-year window reflects the aggressive automation of cybercrime.

- **Financial Impact:** In 2023 alone, cybercrime cases rose by 31.2%, with fraud constituting the majority of these cases. The financial haemorrhage is significant, with the Union Budget 2025-2026 allocating ₹782 crore specifically for cybersecurity projects to stem this tide.

- **Sectoral Vulnerability:** The banking and financial services sector remains the primary target. BioCatch reports that 55% of all fraud in India involves Account Takeover (ATO), where identity theft is the necessary precursor to accessing a victim's funds.

4.1 Typologies of Modern Identity Theft

4.1.1 Financial Identity Theft and the Mule Ecosystem

This is the most prevalent form, involving the theft of PAN, Aadhaar, or credit card details to secure loans or siphon funds. A unique feature of Indian cybercrime is the extensive network of mule accounts bank accounts opened using stolen identities to launder money. It I noted that the devices involved in mule activity in India log into an average of 35 different accounts. This indicates a systemic failure in identity verification processes by banks a processing activity that falls squarely under the DPDP Act's obligations for accurate and secure processing.[9]

4.1.2 Synthetic Identity Theft

[8] Curbing Cyber Frauds in Digital India
[9] BioCatch Releases 2024 Digital Banking Fraud Trends in India, 2025

Here, the thief does not steal a whole identity but fabricates one using a mix of real, stolen Aadhaar number and fake AI-generated face/name information.

- **The Deepfake Challenge:** With the rise of Generative AI, criminals can now bypass Video KYC - Know Your Customer checks. Reports suggest a significant spike in 2024 against deepfake usage for identity fraud, noting that traditional liveness detection is struggling to keep pace.

- **Legal Lacuna:** While the DPDP Act protects personal data, it struggles to address the creation of fake data that mimics real individuals. If a fraudster uses a deepfake of a CEO to order a fund transfer, the line between data protection failure and pure fraud blurs.

4.1.3 Medical Identity Theft

The Star Health data leak serves as a grim reminder of medical identity theft, where stolen health records are used to make fraudulent insurance claims or obtain prescription drugs. This not only causes financial loss to insurers but can corrupt the victim's medical history, leading to life-threatening mistreatment in emergencies.

4.2 Case Studies: The Failures Leading to Regulation

The Hathway Breach (January 2024)

In early 2024, a cybercriminal exploited a vulnerability in the Laravel framework used by Hathway Cable & Datacom Ltd, exposing the personal information of 41 million customers. The compromised data included Aadhaar details, email addresses, and physical home addresses. Under Section 8(5) of the DPDP Act, Hathway would be liable for failing to implement reasonable security safeguards patching the framework. Under Section 8(6), they would be mandated to report this to the Board and every affected user within 72 hours a requirement that forces transparency where opacity was once the norm.

The ICMR Data Leak

Perhaps the most catastrophic breach involved the Indian Council of Medical Research (ICMR), where the personal data of 81.5 crore individuals, including Covid-19 test results and passport details, was allegedly leaked. This breach exposed millions to the risk of identity theft. This case highlights the tension in Section 17 of the DPDP Act. If ICMR is exempted as a government agency in the interest of public health or state security, the victims have no recourse under the DPDP Act, and

the agency faces no penalty. This illustrates the potential for the state to become a super-spreader of identity risk without accountability.

5. COMPARATIVE LEGAL ANALYSIS: DPDP ACT 2023 VS. PREVIOUS REGIMES

5.1 DPDP Act 2023 vs. IT Act 2000 (Section 43A)

The repeal of Section 43A is the most contentious aspect of the new law regarding identity theft. Under the IT Act, if a bank's negligence led to identity theft, the victim could claim compensation directly through an Adjudicating Officer. Under the DPDP Act, the bank pays a fine to the government. The victim is left with a Right to Grievance Redressal but no Right to Compensation within the Act itself. This forces victims to file separate civil suits or consumer court cases to recover financial losses from identity theft, significantly raising the barrier to justice.

5.2 The Criminal Interface: Bharatiya Nyaya Sanhita (BNS) 2023

While the DPDP Act handles data handling, the BNS handles the criminal act of theft and fraud. They operate in tandem to address the full lifecycle of identity theft.

- **Section 319 BNS - Cheating by Personation:** This provision replaces Section 416 of the IPC. It criminalizes the act of pretending to be someone else. This is the primary charge against an identity thief. The imaginary person clause is particularly relevant for synthetic identity theft.
- **Section 336 BNS - Forgery:** This covers the creation of false electronic records. It is crucial for prosecuting crimes where the thief does not just steal data but alters it or creates fake documents digitally.
- **Section 111 BNS - Organized Crime:** The BNS introduces specific provisions for organized crime syndicates. Given that most identity theft operations as organized syndicates, this section allows for stricter bail conditions and harsher sentences for the kingpins of data theft rings.

6. CRITICAL ANALYSIS: GAPS AND VULNERABILITIES

6.1 The Compensation Vacuum

The lack of victim compensation in the DPDP Act is a systemic flaw. Identity theft often results in direct financial loss

and indirect costs legal fees, credit repair, lost wages. By directing all penalties to the state, the Act treats the data as a national asset rather than personal property. This ignores the reality that the harm identity theft is personal. The Internet Freedom Foundation argues this significantly undermines the remedial rights of data principals. Without a simplified compensation mechanism, the average citizen cannot afford to sue a major corporation for a data breach that led to identity theft.

6.2 State Exemptions and Sovereign Immunity

Section 17 grants the government broad powers to exempt its agencies from the Act in the interest of state security or public order. Government databases like Aadhaar, Vahan are the largest repositories of identity data. If these agencies are exempt from strict security safeguards or penalty regimes, they become super-spreaders of identity risks without accountability. The reported CoWin and ICMR breaches highlight this danger. If the state is not held to the same reasonable security safeguards as private entities, the largest vector for identity theft remains unplugged.

7. SUGGESTIONS AND RECOMMENDATIONS

7.1 Reinstating Victim Compensation via Rules

While amending the Act is a legislative hurdle, the government can leverage the Consumer Protection Act, 2019 in tandem with DPDP. The Ministry of Consumer Affairs should notify rules classifying negligent handling of personal data leading to identity theft explicitly as a defective service. This would allow victims to seek compensation in Consumer Commissions, bypassing the lack of remedy in the DPDP Act and utilizing the findings of the Data Protection Board as evidence of deficiency.

7.2 Integrating DPB with Cyber Police (I4C)

Currently, the DPB handles data compliance, and the Police handle identity theft (BNS). There is an operational silo. A formal information-sharing protocol should be established between the Data Protection Board and the Indian Cyber Crime Coordination Centre (I4C). When the DPB receives a breach report under Section 8(6), it should automatically flag it to I4C to watch for spikes in identity theft related to that specific data set. This proactive sharing can help law enforcement anticipate mule account creation waves.

7.3 Mandatory Identity Theft Insurance

Significant Data Fiduciaries (SDFs), particularly in banking and telecom, should be mandated to provide Cyber Insurance

coverage to their customers as part of the reasonable security safeguards. This ensures that if a breach occurs, the customer has financial cover for legal fees and lost funds, even if the Act doesn't provide it directly.

7.4 Enhanced Penalties for Repeat Offenders

The Schedule for penalties should be interpreted to impose the maximum ₹250 crore penalty cumulatively for repeat offenders who fail to rectify security gaps that lead to recurrent identity theft incidents. The Board must use its discretion to ensure that the penalty is not just a cost of doing business but a genuine deterrent.

8. CONCLUSION

The Digital Personal Data Protection Act, 2023, marks a decisive, albeit imperfect, step towards maturing India's digital economy. By imposing high-cost penalties on negligence, it seeks to dry up the supply of stolen data that fuels the identity theft industry. Section 8's security mandates and Section 33's punitive caps effectively serve as a high wall against mass data breaches, forcing corporate India to internalize the cost of cybersecurity.

However, the Act is not a panacea. The repeal of Section 43A of the IT Act leaves a gaping hole in victim remediation, effectively prioritizing state revenue over individual restitution compensation. Furthermore, the extensive state exemptions pose a continued risk of centralized identity theft vectors, and the lack of specific AI regulations leaves the door ajar for synthetic identity fraud.

Ultimately, the fight against identity theft in India will depend on the implementation of the 2025 Rules. If the Data Protection Board acts swiftly, prioritizes the rights of the Data Principal, and imposes deterrent penalties on negligent Fiduciaries, the market will correct itself towards higher security. If it becomes a paper tiger, the digital Indian will remain exposed. The Act provides the shield of data security, but it has removed the sword of civil compensation, leaving the citizen dependent on the vigilance of the state to protect their digital identity.

REFERENCES

1. DeLiema M, Burnes D, Langton L. The Financial and Psychological Impact of Identity Theft Among Older Adults. Innov Aging. 2021 Oct 5;5(4):igab043. doi: 10.1093/geroni/igab043. PMID: 34988295; PMCID: PMC8699092.

2. Reyns BW, Henson B. The Thief With a Thousand Faces and the Victim With None: Identifying Determinants for Online Identity Theft Victimization With Routine Activity Theory. Int J Offender Ther Comp Criminol. 2016 Aug;60(10):1119-39. doi: 10.1177/0306624X15572861. Epub 2015 Mar 2. PMID: 25733745.
3. Guedes I, Martins M, Cardoso CS. Exploring the determinants of victimization and fear of online identity theft: an empirical study. Secur J. 2022 Jul 21:1-26. doi: 10.1057/s41284-022-00350-5. Epub ahead of print. PMID: 40479335; PMCID: PMC9302955.
4. Madriaza P, Hassan G, Brouillette-Alarie S, Mounchingam AN, Durocher-Corfa L, Borokhovski E, Pickup D, Paillé S. Exposure to hate in online and traditional media: A systematic review and meta-analysis of the impact of this exposure on individuals and communities. Campbell Syst Rev. 2025 Jan 16;21(1):e70018. doi: 10.1002/cl2.70018. PMID: 39822240; PMCID: PMC11736891.
5. Dadkhah M, Lagzian M, Borchardt G. Identity Theft in the Academic World Leads to Junk Science. Sci Eng Ethics. 2018 Feb;24(1):287-290. doi: 10.1007/s11948-016-9867-x. Epub 2017 Jan 10. PMID: 28074375.
6. Anderson, Keith B., Erik Durbin, and Michael A. Salinger. 2008. "Identity Theft." Journal of Economic Perspectives 22 (2): 171–192. DOI: 10.1257/jep.22.2.171
7. Vijaya Geeta D (2011), "Online identity theft – an Indian perspective". Journal of Financial Crime, Vol. 18 No. 3 pp. 235–246, doi: https://doi.org/10.1108/13590791111147451
8. Kiran Saini. (2021). Privacy, Identity Theft and Digital Legal Frameworks: An Analytical Study of Laws, Social Media and Technology. International Journal of Engineering, Science and Humanities, 11(4), 21–33. Retrieved from https://www.ijesh.com/j/article/view/42
9. Khan, Md Moeen Ajaz, Identity Theft in India: Legal and Practical Challenges of Aadhaar, PAN, and Bank Details Misuse (September 30, 2025). Available at SSRN: https://ssrn.com/abstract=5550759 or http://dx.doi.org/10.2139/ssrn.5550759
10. Bharati, Dr. Rahul Kailas, Identity Theft and Impersonation in Cyberspace (Sections 66C and 66D of the IT Act, 2000) (July 24, 2025). https://doi.org/10.70593/978-93-7185-183-1, SSRN: https://ssrn.com/abstract=5379783 or http://dx.doi.org/10.2139/ssrn.5379783