CRIMINAL LIABILITY FOR IDENTITY THEFT AND DATA BREACH IN INDIA

AI DISCLOSURE STATEMENT:

"Artificial intelligence tools were used constructively in the preparation of this work specifically to check grammatical errors, improve sentence structure and clarity and assist with the accurate formatting of citations and references. All intellectual content, arguments, and conclusions remain solely those of the authors."

Abstract

The Rapid advancements in technology have transformed the processing, storage, transfer, and use of personal data, making data protection a critical legal concern. While digital governance, online banking, and e-commerce have accelerated economic growth, they have also increased cybercrimes such as identity theft, ATM skimming, unauthorized access, and data breaches causing significant financial and reputational harm.

Although the right to privacy has been recognized as a fundamental right under Article 21 of the Constitution of India, the legal framework governing criminal liability for data theft remains fragmented. Criminal offences are addressed under the Information Technology Act, 2000 and the Bharatiya Nyaya Sanhita, 2023, while the Digital Personal Data Protection Act, 2023 primarily establishes a regulatory framework.

This paper critically examines India's legal regime on criminal liability for data theft and data breaches through constitutional principles, cyber laws, and recent developments. It also compares the Indian framework with international data protection standards and proposes reforms to create a coherent legal framework integrating criminal sanctions with regulatory compliance, thereby strengthening data security, accountability, and public trust in the digital ecosystem.

Keywords: Data Breach; Identity Theft; Digital Personal Data Protection Act, 2023; Criminal Liability.

I. INTRODUCTION:

"There are only two types of companies in the world: those that have been breached and know it and those that have been breached and don't know it." – Ted Schlein[1]

Technology has seen tremendous unprecedented progress in last decade to bring about sweeping changes in every walk of life of an individual-whether it is the way people communicate, carry on trade and business, avail public service or exchange information. Among all such significant technological advances, computer and information & communication technologies (ICT) has witnessed exponential growth for enabling to compute, store and transmit huge quantity of data within a blink of an eye. Further, with the advent of Internet and interoperable digital networks has facilitated the advent of Cyberspace, a virtual environment consisting of computers, mobile devices, software and telecommunication networks linked through electronic and optical signals.

EVOLUTION OF THE DIGITAL ECONOMY:

India has seen significant digital change through initiatives like Digital India. This program aims to promote digital governance, financial inclusion, and technology-driven public services. The introduction of the Aadhaar system, the world's largest biometric identification system, has made it easier to deliver welfare programs, verify digital identities, and access banking and government services smoothly. At the same time, the rapid growth of digital banking and the Unified Payments Interface (UPI) has changed how people handle money by enabling secure, real-time payments and reducing reliance on cash. The rise of e-commerce platforms has also reshaped consumer markets by allowing businesses to connect with customers across different regions.

Meanwhile, cloud computing has helped organizations store, process, and manage large amounts of data more effectively and at a lower cost. All these changes have boosted economic growth and solidified India's status as one of the fastest-growing digital economies in the world. However, the growing accumulation of valuable personal and business data in digital systems has created new risks that cybercriminals can exploit.

[1] RSA Security conference panel

"The supreme court unanimously ruled in *Justice K.S. Puttaswamy v. Union of India (2017)*[2] that the right to privacy is fundamental right under Article 21." The bench explicitly detailed that "informational privacy" and bodily/digital autonomy are vital. This judgment forms the complete constitutional bedrock for prosecuting biometric data leaks, synthetic profiling and unauthorized identity trades.

II. RISE OF IDENTITY THEFT, DATA BREACHES AND EMERGING CYBERCRIMES

The rapid digitization of governance, commerce, banking, healthcare, education, and communication has significantly changed how personal information is created, stored, processed, and exchanged. Data has become one of the most valuable assets in the digital economy. It is often referred to as the "new oil" because of its great commercial, strategic, and economic value. Initiatives like Digital India, the Aadhaar ecosystem, Unified Payments Interface (UPI), Digi Locker, e-governance platforms, online banking, and cloud-based services have sped up India's shift toward a digitally empowered society. While these tech advancements have improved financial inclusion, administrative efficiency, and economic growth, they have also opened new opportunities for cybercriminals to take advantage of flaws in digital systems. As a result, identity theft, data breaches, and cyber-enabled financial crimes have surged, posing serious threats to privacy, cybersecurity, and national security.

IDENTITY THEFT:

'Identity' is a proof of one's existence and 'theft' is to have the possession of a property which does not belong to you or without the consent of the owner. Thus, 'identity theft' is a theft in which the possessor of another's identity does not own it.
As stated by **Black's law dictionary**[3], 'Identity theft is the unlawful taking and use of another person's identifying information for fraudulent purpose'.

[2] AIR 2017 SC 4161
[3] *Identity Theft*, Black's Law Dictionary (12th ed. 2024).

“Identity theft is a product of deliberate carelessness. The reason so much identity theft occurs is because it is cheaper to expose people to the risk of identity theft than to exercise more care...”— **Daniel J. Solove and Woodrow Hartzog**[4]

Identity theft involves the unauthorized acquisition and fraudulent use of someone else's personal information. This includes Aadhaar numbers, Permanent Account Numbers (PAN), passwords, banking credentials, biometric data, digital signatures, or One-Time Passwords (OTPs). Thieves use this information to impersonate the victim and gain unlawfully. They might obtain unauthorized loans, withdraw money, commit online fraud, create fake identities, or carry out illegal financial transactions.

Vilas Prabhakar Lad v. UIDAI & Ors (Bombay High Court, 2025)[5] The Bombay High Court ruled that regulatory bodies and agencies like UIDAI must act to protect citizens from identity theft. It heavily criticized statutory authorities for their apathy and mandated that they take corrective action to redress grievances caused by identity misuse

When identity theft moves beyond basic credit card fraud, it branches out into several specialized and often more complex categories.

Extended branches of identity theft:

1. Synthetic Identity Theft

Instead of stealing a single person's complete identity, fraudsters blend real information (like a legitimate Social Security number or national ID) with completely fabricated data (like a fake name and date of birth). This creates a "synthetic" person used to open fraudulent bank accounts or build credit lines over time before disappearing.

2. Criminal Identity Theft

This occurs when a criminal uses another person's name and personal details (often via a stolen driver's license or fake ID) during an arrest or citation. If successful, the legal charges, warrants, and criminal records end up under the innocent victim's name, often discovered only during a background check.

3. Identity Cloning and Concealment

[4] Daniel J. Solove & Woodrow Hartzog, Breached! Why Data Security Law Fails and How to Fix It (Chapter 10, "Data Breach Harms and Inadequate Cures"), Oxford University Press, 2022
[5] 2025 SCC OnLine Bom 2724

The thief completely assumes the victim's identity in their daily life. This branch is typically used by individuals hiding from law enforcement, evading debts, or seeking to establish an unauthorized legal status in a country, allowing them to blend into society indefinitely.

4. Tax Identity Theft

Fraudsters use a victim's personal identification number to file a fraudulent tax return early in the tax season and pocket the government refund. Victims typically only discover this when their legitimate tax return is rejected as a duplicate.

5. Child Identity Theft

Cybercriminals target the clean, unmonitored credit profiles of minors. Because children don't check their credit reports or apply for loans, a thief can exploit a child's ID for years. The crime is usually only discovered when the victim grows up and applies for a student loan or first credit card.

DATA BREACH: A GROWING CYCLE

Data breaches have become one of the biggest threats to informational privacy, cybersecurity, and public trust in digital governance. Just one data breach can expose millions of people to identity theft, financial fraud, cyber extortion, reputational damage, and misuse of sensitive personal information.

At its core, a data breach means any event where personal or confidential information, stored either digitally or physically, is accessed, acquired, disclosed, altered, destroyed, lost, or misused without authorization.

At the international level, the concept of a data breach has been comprehensively recognized under the **General Data Protection Regulation (GDPR)[6] of the European Union**. **Article 4(12)** of the GDPR defines a **"personal data breach"** as:

"A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored or otherwise processed."

[6] Regulation (EU) 2016/679

In India, the **Digital Personal Data Protection Act, 2023 (DPDPA)** expressly recognizes the concept of a data breach for the first time in a comprehensive data protection legislation. **Section 2(u)** of the Act defines a **"personal data breach"** as:

"Any unauthorised processing of personal data or accidental disclosure, acquisition, sharing, use, alteration, destruction or loss of access to personal data that compromises the confidentiality, integrity or availability of personal data."

Stolen databases with customer records, healthcare information, financial details, intellectual property, or government documents are often sold on underground marketplaces on the Dark Web. This hidden part of the internet requires special software for anonymous communication and illegal trade in stolen data, malware, and hacking tools.

Generative AI Exploits: Cybercriminals use AI to automate hyper-personalized phishing campaigns, clone voices for social engineering, and rapidly exploit zero-day vulnerabilities.

Deepfake Proliferations: Sophisticated video and audio deepfakes fool biometric security systems and verification protocols employed by banks and government agencies.

A major banking liability *(Dhule Vikas Sahakari Bank v. AXIS Bank (2025)*[7]*)* where a security compromise led to massive financial diversion. An Administrative Adjudication under section 43A of the IT Act highlighted rigorous bank accountability when dealing with technological fraud vectors and systemic security oversights.[8]

Ransomware & Double Extortion: Cybercriminals not only lock down corporate systems, they also threaten to expose sensitive, stolen consumer data on the dark web if payment is not made.

Historically significant as India's first cybercrime conviction *(State of Tamil Nadu vs Suhas Katti (2004)*[9]*)* dealing with identity defacement and digital impersonation under section 67 of the IT act. It establishes how electronic trails and IP tracking must be handled by Indian trial courts.

[7] Complaint No.03 of 2019 (Adjudicating Officer under IT Act, Maharashtra, Jan.21,2025(India)
[8] https://www.prashantmail.com/cyber-law-blog-india/important-cyber-law-case-laws-in-india
[9]CC No. 4680 of 2004

RECENT DATA BREACH INCIDENT:

Nuclear Power Plant Blueprint Leak[10]: The ransomware group "World Leaks" posted over 19,000 files stolen from a contractor (Reliance Infrastructure). The leak included ventilation blueprints, control room layouts, supplier lists, and inspection reports. India's CERT-In is currently investigating the physical and supply chain security risks.

Tata Electronics Supply Chain Exposure[11]: The same group published 630 GB of internal documents from Tata Electronics (a manufacturer for Apple and Tesla). The data exposed factory operating procedures, component specs, and internal emails, risking global supply chain safety. Tata has restricted network access and launched a forensic audit.

In light of these challenges, India has introduced significant legislative measures like the Digital Personal Data Protection Act, 2023 (DPDPA) to regulate collection, processing, storage and protection of personal data.

III. Constitutional Basis of Data Privacy in India

Data privacy is a subject of significant importance in India, due to rapid economic digitalization and cyber threat increase. Even though Indian Constitution did not refer to personal data yet, the articles established in Constitution offer to protect the private data. The data privacy in India section describes some legal bases of data privacy, that include the elements of judiciary and laws that are the means to guard personal data.

Article 21: No person shall be deprived of his life or personal liberty except according to the procedure established by law.

R. Rajagopal v. State of Tamil Nadu (1994)[12] (The Auto Shankar case) the Supreme Court upheld right to privacy under Article 21 as the fundamental right[13] when deciding an issue relating to law of unauthorised disclosure of information relating to private life of any individual.

---

[10] *Files Relating to India's Largest Nuclear Power Plant Kudankulam Exposed in Data Breach*, REUTERS (July 15, 2026), reuters.com.
[11] *India's Tata Electronics Hit by Cyber Breach Claiming to Expose Apple, Tesla Trade Secrets*, REUTERS (June 22, 2026), https://www.reuters.com/business/media-telecom/indias-tata-electronics-hit-by-cyber-breach-claiming-expose-apple-tesla-trade-2026-06-22/.
[12] AIR (1994) 6 SCC 632.
[13] Puttaswamy, (2017)10 SCC 1 (India)

Article 19: Protection of Certain Rights regarding Freedom.

Article 19(1)a: All citizens shall have the right to freedom of speech and expression. Article 19(1)g: All citizens shall have the right to practice any profession, or to carry on any occupation, trade or business. Data Privacy: Freedom of expression and right to run a business intersect data privacy, due to the fact that the right to express views should be balanced against the right to privacy, while unauthorised disclosures of personal information can be privacy invasions.

Data privacy laws must not be discriminatory and must apply equally to all individuals and organizations. Data privacy regulations should be just, equitable, and rational, extending equal protection to all individuals. The decisions of the Supreme Court, particularly those that affirm privacy as a fundamental right under Article 21, and impose strict conditions of legality, reasonableness, and proportionality, have significantly shaped data protection in India.

In addition, other provisions like Articles 19, 14, and 32 contribute to the overall framework by safeguarding the right to express oneself, ensuring equality before the law, and providing legal recourse against privacy violations through public interest litigations.

IV. Digital Personal Data Protection Act, 2023

The Digital Personal Data Protection Act 2023 is a step forward for India's data protection rules. It sets out duties for companies that handle data to keep it safe and report any major data breaches to the Data Protection Board of India.

However, the Act mainly focuses on fines and following rules. It does not make Cyber Crimes like hacking, data theft or ransomware attacks punishable by criminal law.

This means that serious Cyber Crimes are still covered by laws like the Information Technology Act, 2000 and the Bharatiya Nyaya Sanhita, 2023. This creates a situation where different laws apply depending on the type of Cyber Crime.

Fragmented Criminal Framework and Absence of Specific Offence of Data Theft

One major problem in India is that there is no law that deals with data theft. The Information Technology Act, 2000 does provide some protection against Cyber Crimes. It does not cover all types of data theft.

Some important parts of the Act include:

Section 43 – Unauthorized access, downloading, copying, or extraction of data from computer systems.

Section 66 – Criminal liability for computer-related offences committed dishonestly or fraudulently.

Section 66C – Identity theft involving misuse of passwords, digital signatures, or unique identification information.

Section 66D – Cheating by personation using computer resources (section 319 BNS[14])

Section 66E – Violation of privacy through capturing, publishing, or transmitting private images.

Sections 72 and 72A – Breach of confidentiality and disclosure of information without lawful authority.

While famous for striking down section 66A of the IT Act due to overbreadth, this judgment *(Shreya Singhal v. Union of India (2015)[15])* firmly established the baseline for intermediary liability (section 79). It dictates exactly how and when online platforms must take down malicious content once notified by a court order or government agency, which is heavily used today to force the deletion of deepfakes and leaked data.

However new crimes like AI-generated identity fraud and large-scale data scraping are not fully covered by these rules.

Challenges in Investigation and Electronic Evidence:

Investigating crimes is hard because digital evidence can be easily changed or deleted. Cyber criminals often use technologies like private networks and cryptocurrencies to hide their identities.

The Supreme Court has emphasized the importance of keeping evidence authentic and reliable.

[14]Bharatiya Nyaya Sanhita ,2023
[15] (2015) 5 SCC 1 (India)

Protecting personal data is closely linked to the right to privacy. The Supreme Court has recognized privacy as a right. However, investigating crimes often requires access to personal data. A balance must be struck between investigating crimes and protecting privacy.

V. Comparative Analysis between GDPR and DPDP Act:

The overarching aim behind both the European Union's General Data Protection Regulation and the Digital Personal Data Protection Act, 2023 of India is to safeguard personal data of individuals and govern its use in this digital age. However, due to their underlying socio-political, legal, and economic conditions, the coverage and operative features of the frameworks are disparate. The GDPR, a comprehensive regulatory framework, has significant extraterritorial reach and serves as a developed and evolved data protection regime.

On the contrary, the DPDP Act is India's inaugural robust attempt to control digital personal data. This came into existence following the constitutional recognition of the Right to Privacy in the case of Puttaswamy[16]. There is a huge similarity and difference in several spheres like the scope of data, conditions for obtaining the consent, category of rights of an individual, the legal duty of entities handling the data, the process of enforcement and regulating international data transfer.

Scope and Applicability: The GDPR has been characterized by its expansive and intentional broad coverage because of its structured nature. The processing of personal data that involves either entirely or partly automatic processes, and the manual processing of personal data when it is organized into a filing system falls under the preview of the GDPR. The GDPR's geographical reach extends beyond the European Union, thus controlling the non-EU entities for the purposes of goods and services to individuals located in the European Union or tracking them, within the EU territory.

Moreover, personal data according to the GDPR refers to all data relating to any identified or identifiable natural person. The scope of GDPR also covers a broad list of "special categories of personal data" such as race or ethnic origin, political opinions, religious and other beliefs,

[16] AIR 2017 SC 4161 (India)

union membership, genetic data, biometric data for identification, health information and sexual life or orientation data, all of which have enhanced protection guidelines.

VI. Proposed reforms in India's Legal Framework for Criminal Liability in Identity Theft and Data Breach

The increasing sophistication of cybercrime such as identity theft, mass data breaches, AI impersonation, deepfake fraud and cryptocurrency offences, substantial reforms in India's criminal law are warranted. While the Information Technology Act, 2000 (IT Act), the Bharatiya Nyaya Sanhita, 2023 (BNS) and the Digital Personal Data Protection Act, 2023 (DPDP Act) provide a basic framework for regulating cyber offences, they need to be modernized to cater to contemporary technological challenges.

The following reforms can strengthen criminal liability for identity theft and data breaches, and improve protection of digital identities:

1. **Comprehensive, Technology-Neutral Cybercrime Legislation:** India enacted the IT Act in an era when cyber-threats were relatively nascent. Modern cyber-offences like AI-driven identity fraud, deepfake impersonation, biometric identity theft, synthetic identities, and blockchain-based crimes demand a contemporary and technologically neutral legal framework that captures such activities irrespective of the technology employed.
2. **Dedicated Cybercrime Courts:** To facilitate expeditious trial of complex digital cases, dedicated cybercrime courts or specialised cyber-benches with judges knowledgeable about digital forensics and technology are necessary. This would improve consistency in judicial outcomes and increase the conviction rate.
3. **Enhancing Digital Forensics Infrastructure and Electronic Evidence Framework :** The ability to gather and present admissible electronic evidence is crucial for successful prosecution of cybercrimes. Investment in digital forensic laboratories, standardized protocols for data acquisition and analysis, and training for law enforcement personnel in forensic investigation, and for judges and prosecutors on evaluating electronic evidence under the Bharatiya Sakshya Adhiniyam, 2023 would enhance effectiveness.
4. **Criminal Liability for Serious Corporate Negligence while handling data:** As primarily an administrative regime for data breaches, the DPDP Act could benefit from

the introduction of criminal liability for corporations that demonstrably fail to protect data due to wilful negligence or egregious disregard for security obligations, leading to mass data breaches or identity theft. This would create stronger accountability for organizations.

5. **Strengthened Victim Protection and Compensation Schemes:** A legal framework for identity theft and data breaches should include provisions for effective and swift compensation to victims, both during and post criminal proceedings. This can be facilitated by a dedicated victim compensation fund, potentially financed by regulatory penalties levied on organisations found guilty of data security lapses.
6. **Improve Cross-Border Enforcement and International Cooperation:** Cybercriminals often operate beyond India's borders, thus necessitating closer international collaboration. Strengthened mutual legal assistance treaties, bilateral extradition agreements, participation in international forums, and effective information-sharing arrangements with foreign law enforcement agencies would bolster cross-border investigations and prosecutions.
7. **Enhanced Accountability for Intermediaries and Platforms:** Intermediaries, social media companies, cloud providers, and digital platforms should be equipped with robust identity verification measures, clear protocols for reporting incidents, effective data management practices, and close cooperation with law enforcement. However, intermediary responsibilities must not impinge on constitutionally protected rights like freedom of speech and privacy.

VII. Conclusion

A robust legal regime for identity theft and data breaches requires not only punitive measures but a multi-faceted approach that includes substantive criminal law, robust procedure, advanced forensics, effective regulatory oversight, victim compensation and international cooperation. Reforming India's cyber laws to align with technological progress and international best practices is essential for deterring and prosecuting these modern cybercrimes while safeguarding the citizens' rights to privacy, dignity, and informational autonomy.

BIBLIOGRAPHY

A. Statutes

1. Constitution of India, 1950.
2. Bharatiya Nyaya Sanhita, 2023.
3. Bharatiya Sakshya Adhiniyam, 2023.
4. Information Technology Act, 2000.
5. Digital Personal Data Protection Act, 2023.
6. Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011.

B. Cases

1. *Justice K.S. Puttaswamy (Retd.) v. Union of India*, (2017) 10 SCC 1.
2. *Shreya Singhal v. Union of India*, (2015) 5 SCC 1.
3. *R. Rajagopal v. State of Tamil Nadu*, (1994) 6 SCC 632.
4. *State of Tamil Nadu v. Suhas Katti*, C.C. No. 4680 of 2004.
5. *Vilas Prabhakar Lad v. UIDAI*, 2025 SCC OnLine Bom 2724.
6. *Dhule Vikas Sahakari Bank Ltd. v. AXIS Bank Ltd.*, Complaint No. 03 of 2019 (Maharashtra Adjudicating Officer, IT Act, 2025).

C. Books

1. Daniel J. Solove & Woodrow Hartzog, Breached! Why Data Security Law Fails and How to Fix It (Oxford University Press, 2022).
2. Black's Law Dictionary (12th ed., Thomson Reuters, 2024).
3. Pavan Duggal, Cyber Law: The Indian Perspective (latest ed.).
4. Justice Yatindra Singh, Cyber Laws (Universal Law Publishing, latest ed.).

D. Reports

1. Justice B.N. Srikrishna Committee, *A Free and Fair Digital Economy: Protecting Privacy, Empowering Indians* (2018).
2. Ministry of Electronics and Information Technology, *Digital Personal Data Protection Act, 2023*.

3. National Crime Records Bureau, *Crime in India* (Cyber Crime Chapter).

E. Websites

1. Ministry of Electronics and Information Technology (MeitY), Government of India – https://www.meity.gov.in
2. Supreme Court of India – https://www.sci.gov.in
3. India Code – https://www.indiacode.nic.in
4. Reuters – https://www.reuters.com (for recent cyber breach reports)
5. European Union – https://eur-lex.europa.eu (GDPR)

F. Online Databases

1. SCC Online.
2. Manupatra.
3. LexisNexis India.
4. Westlaw.