



# DATA THEFT AS AN EMERGING CRIME IN INDIA; A CRITICAL ANALYSIS OF LEGISLATIVE FRAME WORK

VAISHNAVI M 1, Dr. SUNOWAR AMEER 2

LLM Student, School of Law, Lovely Professional University, Punjab, India 1

Assistant Professor: LAW-I, School of Law, Lovely Professional University, Punjab, India 2

School Of Law 1

Lovely Professional University, Punjab, India 1

**Abstract:** Data theft is emerging as a big issue in India's digital world, affecting people, businesses, and the countries security in India there are two Acts plays an important role in controlling data privacy problems; the Information Technology Act 2002 and Digital Personal Data Protection Act 2023. This paper critically analyzes the legislative framework surrounding data protection in India, with a focus on its effectiveness in addressing the growing threat of data theft. Through a thorough examination of relevant laws, regulations, and enforcement mechanisms, the study identifies strengths and weaknesses in the current legal framework. By studying all of this, the paper suggests ways to make the laws better and keep data safer in India.

**Index Terms:** Data theft, Cybercrime, Legislative Framework

## 1. INTRODUCTION:

Recent years have seen an unparalleled increase in connectivity, communication, and commerce because to the spread of digital technology and the internet's quick growth. But there are also new difficulties brought about by the digital revolution, the most significant of which is the growing risk of data theft. In the nation of India, which is undergoing its own digital revolution, data theft has become a major issue with broad consequences for people, companies, and the society at large.

Examining the causes, effects, and effectiveness of the current legal framework in managing this dynamic danger, this research study aims to investigate the topic of data theft in the Indian context. This research attempts to illuminate the advantages and disadvantages of the existing legal framework in preventing data theft by critically examining the pertinent laws, rules, and enforcement practices. Moreover, it will examine possible directions for development and give suggestions for legislators to fortify India's data protection laws and regulations.

Upon closer examination of this intricate and diverse matter, it is apparent that a thorough comprehension of the technological, legal, and socio-economic aspects involved is important for the efficient management of data theft. This research study seeks to further the existing conversation in India about data security and privacy by doing this essential analysis, eventually working toward a more secure and safe digital environment for all parties involved.

### 2.1 THE INFORMATION TECHNOLOGY ACT, 2000 (IT ACT)

- i. The principal legal framework in India for dealing with cybercrime, including data theft, is the Information Technology Act, 2000 (IT Act). Important clauses include:

- ii. Section 43, which prosecutes unauthorized users who destroy computer systems.
- iii. A fine of up to ₹5 lakh and three years in jail are the penalty for cybercrimes including hacking and data theft under Section 66.
- iv. A punishment of up to ₹1 lakh and three years in jail are the penalties under Section 66B, which deals with the fraudulent reception of stolen communication equipment or computer resources.
- v. A punishment of up to ₹1 lakh and three years in jail are the penalty for identity theft under Section 66C, which targets the impersonation of digital signatures or other distinctive identification traits.

### **3.1 THE PERSONAL DATA PROTECTION ACT 2023**

Data theft is specifically addressed by the Personal Data security Act 2023 in India, which addresses problems like identity theft and data breaches and creates a strong framework for data security. Financial loss, identity theft, and reputational impairment are among the categories of harm caused by breaches, and reporting of any personal data breach to the Data Protection Authority is required.<sup>1</sup>The Act further provides the Data Protection Board the power to take immediate corrective action in the event of a breach and specifies fines for non-compliance that range from INR 500 million to INR 2.5 billion. By preventing illegal access and exploitation of personal information, including data theft, this act marks a major advancement in data security.<sup>2</sup>

#### **4.1 SECTOR SPECIFIC REGULATIONS**

- i. Within two to six hours, banks and other financial institutions are required by the Reserve Bank of India to disclose cybersecurity issues.
- ii. Insurance companies are also required by the Insurance Regulatory and Development Authority to report such instances to the agency within 48 hours.
- iii. Telecom providers are mandated by the Telecom Regulatory Authority of India to notify of any breaches.

#### **5.1 JUDICIAL INTERVENTION**

- i. **Justice K.S. Puttaswamy (Retd.) & Anr. v. Union of India & Ors. (2017):<sup>3</sup>**

The Supreme Court of India rendered a historic decision in the Aadhaar case, which established the right to privacy as a basic freedom guaranteed by the Indian Constitution. The necessity of shielding private information from abuse and illegal access was underlined.

- ii. **State of Tamil Nadu v. Suhas Katti (2018):<sup>4</sup>**

In this instance, a person was found guilty by the Madras High Court of breaking into the website of the Tamil Nadu e-Governance Agency and wiping confidential government information. Legal ramifications of illegal access to digital data were brought to light by this case.

- iii. **Rajasthan Royals v. BCCI & Ors. (2014):<sup>5</sup>**

In this instance, private team information from the Indian Premier League (IPL) was unlawfully accessed and disclosed. It brought up concerns about digital platforms and sports leagues as well as data security and intellectual property rights.

<sup>1</sup> Available at;<https://prsindia.org/billtrack/digital-personal-data-protection-bill-2023>(last seen at 25 may 2024)

<sup>2</sup> Available at;<https://www.lw.com/admin/upload/SiteAttachments/Indias-Digital-Personal-Data-Protection-Act2023-vs-the-GDPR-A-Comparison.pdf> (last seen at 25 may 2024)

<sup>3</sup> Justice K.S. Puttaswamy (Retd.) & Anr. v. Union of India & Ors. (2017)

<sup>4</sup> State of Tamil Nadu v. Suhas Katti (2018)

<sup>5</sup> Rajasthan Royals v. BCCI & Ors. (2014)

iv. **Shreya Singhal v. Union of India (2015):**<sup>6</sup>

Although not specifically connected to data theft, the lawsuit addressed the constitutionality of Section 66A of the Information Technology Act, which was utilized to censor online expression. The ruling underscored the need of striking a balance between the right to free expression and the necessity of efficiently regulating the internet, which has an indirect bearing on data protection.

v. **The Subhranshu Rout and Gugul v. State of Odisha Case**<sup>7</sup>

Highlights the imperative need to address privacy concerns in the contemporary digital age. The case underscores the significance of legal frameworks that embrace ideas such as the "right to be forgotten" and effectively handle issues like online defamation and privacy protection by recognising the victim's right to privacy and encouraging measures to protect them online.

vi. **In the Balu Gopalakrishnan v. State of Kerala Case**<sup>8</sup>

The COVID-19 data transmission to a US-based business for analytics purposes was considered by the Kerala High Court. After the COVID-19 outbreak, the court emphasized the need to set standards for data privacy in public-private partnerships by putting measures in place before approving such transfers. In partnerships involving sensitive information, this instance demonstrated the need for stringent data protection procedures.

## 6.1 THE IMPACT OF DATA THEFT

i. Impact on Individual;

It causes financial losses, identity theft, credit monitoring, and credit rehabilitation for individuals by compromising their personal and financial information. This might affect career opportunities as well as cause mental distress and a lack of faith in the firms that store their data.<sup>9</sup>

ii. Impact on business;

In addition to response expenses, lawsuit settlements, and reputational harm, businesses must contend with significant financial obligations that can result in dwindling sales, eroded market value, and a loss of consumer confidence. Investments in cybersecurity are also more urgently needed, and risk management procedures need to be adjusted. On credit ratings and cash flow stability, these changes may have long-term implications.<sup>10</sup>

iii. Impact on economy

Broadly speaking, data breaches result in large financial losses; on average, \$3.86 million is lost every occurrence.<sup>11</sup> In extreme situations, these costs may cause major disruptions to vital services and infrastructure, which often results in increased pricing for consumers. They also erode customers' trust in online shopping and digital transactions.

In essence, addressing data theft necessitates a comprehensive legislative framework and robust cybersecurity measures to mitigate its widespread impact

## 7.1 IDENTIFICATION OF GAPS OR SHORT COMINGS IN CURRENT LAWS AND REGULATIONS

<sup>6</sup> Shreya Singhal v. Union of India (2015)

<sup>7</sup> The Subhranshu Rout and Gugul v. State of Odisha

<sup>8</sup> In the Balu Gopalakrishnan v. State of Kerala

<sup>9</sup> economic costs and impacts of business data breaches by Ping Wang, Robert Morris University, wangp@rmu.edu Hubert D'Cruze, University of Maryland, hubert.dcruze@yahoo.com David Wood, Robert Morris University, [wood@rmu.edu](mailto:wood@rmu.edu)(last seen at 25 may 2024)

<sup>10</sup> The economic impact of data security breaches in e-commerce by Satta Sarmah Hightower(last seen at 28 may 2024)

<sup>11</sup> Available at; <https://www.verizon.com/business/resources/articles/s/economic-impact-of-data-security-breaches-in-ecommerce/>(last seen at 28 may 2024)

The assessment of deficiencies in current Indian laws concerning data theft highlights significant problems within the legal structure:

i. Insufficient Legal Infrastructure:

In order to address the evolving nature of cybercrimes like data theft, the existing legal framework—most notably the Information Technology Act of 2000—is judged insufficient. A lack of comprehensive protections aimed at protecting data and privacy is perceived in these regulations as their generality and fragmentation.<sup>12</sup>

ii. Absence of Holistic Data Protection Legislation:

Policies like the Digital Personal Data Protection Act of 2023 are a start, but more comprehensive laws are still needed to protect data subjects' rights and to make it illegal to use gathered data for uses other than those for which it was intended.

iii. Difficulties in International Collaboration:

One of the biggest challenges to effectively resolving cases involving cross-border cyber offenses is the lack of a consistent legal framework for dealing with crimes committed abroad. Investigating and prosecuting cybercriminals who operate across borders is made more difficult by this obstacle.

iv. Rapid Technological Progress and Encryption Tools:

It is difficult to trace down and prosecute cyber criminals because they use encryption methods to conceal data and evade law enforcement. Due to the ability of criminals to conceal their identities, technologies like the Darknet complicate investigations and highlight the need for enhanced skills to counter sophisticated cyber threats.

v. Resource Limitations and Limited Awareness:

Because there are limited resources and inadequate knowledge to identify and respond appropriately to cyber threats, both individuals and businesses are vulnerable to cyberattacks. To create a safer online environment and raise the success rate of cybercrime prosecutions, it is imperative to raise awareness, enforce data protection laws, and strengthen cybersecurity infrastructure.

## **8.1 CRITICAL ANALYSIS OF LEGISLATIVE FRAMEWORKS**

### **8.1.1 STRENGTHS;**

i. Broad Scope of the IT Act<sup>13</sup>

**Extensive Coverage:** The Information Technology Act, 2000 (IT Act) addresses a wide variety of cybercrimes, including data theft, hacking, and unauthorized data access, providing a solid legal basis for addressing these issues.

**Ongoing Amendments:** The IT Act has been updated to include new forms of cybercrime, reflecting the latest technological advancements and emerging threats. Notably, the IT (Amendment) Act, 2008 introduced specific provisions to enhance data protection and privacy.

ii. Sector-Specific Data Protection Regulations<sup>14</sup>

<sup>12</sup> Available at: <https://juriscentre.com/2021/05/28/law-regarding-data-theft-in-india/> (last seen at 28 may 2024)

<sup>13</sup> Available at: <https://blog.ipleaders.in/critical-analysis-cybercrime-india/> (last seen at 30 may 2024)

<sup>14</sup> Available at: <https://www.mondaq.com/india/data-protection/1378424/corporate-data-theft-a-major-concern> (last seen at 28 may 2024)

Financial Sector: The Reserve Bank of India (RBI) has established guidelines to ensure robust data protection and cybersecurity measures within the banking sector.

Telecommunications: The Telecom Regulatory Authority of India (TRAI) has implemented regulations aimed at safeguarding consumer data and securing telecom networks.

Healthcare: Emerging regulations are increasingly focused on protecting health data, ensuring compliance with established data protection standards.

### iii. Judicial Contributions<sup>15</sup>

Influential Rulings: Indian courts have interpreted data protection laws in ways that strengthen the legislative framework. Key judgments have underscored the importance of data privacy and protection, thus reinforcing legislative intent.

## 8.1.2 WEAKNESSES;

### i. Insufficient Current Laws: <sup>16</sup>

-Existing laws do not adequately cover all aspects of data protection, such as consent management, data minimization, and the rights of data subjects, which are essential for comprehensive data protection.

### ii. Ambiguities in Legal Provisions<sup>17</sup>

- Unclear Definitions: Some terms and provisions within the IT Act and related regulations are ambiguously defined, leading to interpretational challenges and inconsistent application.

- Jurisdictional Overlaps: Conflicting provisions and overlapping jurisdictions among various regulations can create confusion and hinder effective enforcement.

### iii. Challenges in Addressing International Data Theft

- Jurisdictional Complications: Cybercrimes often have cross-border elements, complicating jurisdictional issues and enforcement. The current legal framework struggles to manage the complexities of international data theft and collaboration.

- Limited Global Cooperation: Inadequate international cooperation and inconsistent global data protection standards impede efforts to address cross-border data theft effectively.

### iv. Low Public Awareness and Cyber Hygiene<sup>18</sup>

- Insufficient Awareness Campaigns: There is a lack of comprehensive public awareness campaigns on data protection and cybersecurity best practices, leaving individuals and organizations more susceptible to data breaches.

- Insider Threats and Negligence: Insider threats and negligence continue to be significant challenges, as many data breaches result from a lack of awareness and poor cybersecurity practices within organizations.

<sup>15</sup> Available at: <https://www.legalserviceindia.com/article/I267-Data-Theft-in-Cyber-Space.html> (last seen at 28 may 2024)

<sup>16</sup> Available at: <https://www.jsalaw.com/newsletters-and-updates/stringent-measures-against-cybercrimes-in-indias-new-criminal-justice-system/> (last seen at 28 may 2024)

<sup>17</sup> Available at: [https://indraprasthalawreview.in/wp-content/uploads/2020/10/ggsipu\\_uslls\\_ILR\\_2020\\_V1-I1-13-aditi\\_palit-abhishek\\_kushwaha.pdf](https://indraprasthalawreview.in/wp-content/uploads/2020/10/ggsipu_uslls_ILR_2020_V1-I1-13-aditi_palit-abhishek_kushwaha.pdf) (last seen at 28 may 2024)

<sup>18</sup> Available at: <https://www.jsalaw.com/newsletters-and-updates/stringent-measures-against-cybercrimes-in-indias-new-criminal-justice-system/> (last seen at 28 may 2024)

Enhancing these weaknesses and building upon the strengths will help India create a more robust legislative framework to combat data theft and protect personal and organizational data.

## **9.1 RECOMMENDATIONS**

### **i. Enhancing Enforcement Mechanisms**

- Establishing specialized cybercrime units
- Training law enforcement personnel in cyber forensics

### **ii. Public Awareness and Education**

- Promoting cybersecurity hygiene among individuals and organizations
- Encouraging responsible data handling practices

### **iii. International Cooperation**

- Collaborating with global entities to tackle cross-border data theft
- Adopting best practices from international data protection regimes

## **10.1 CONCLUSION**

Data theft is undoubtedly an escalating concern in India, with its multifaceted implications spanning individual privacy infringements, economic repercussions, and business vulnerabilities. A critical examination of the legislative framework reveals a promising trajectory, notably with the enactment of the Information Technology Act 2000 and the subsequent introduction of the Personal Data Protection Act 2023, alongside sector-specific regulations. However, despite these legislative efforts, significant gaps persist, necessitating urgent attention.

The impact of data theft on individuals is profound, eroding trust and exposing them to various forms of exploitation. Economically, the repercussions are far-reaching, undermining investor confidence, hindering innovation, and impeding growth. For businesses, data theft represents a tangible threat to competitiveness and sustainability, with potential reputational damage and financial losses looming large.

Judicial intervention has been instrumental in interpreting and enforcing existing laws, yet challenges persist in investigating data theft cases, ranging from the complexity of cyber forensics to jurisdictional issues and resource constraints. Addressing these challenges demands a concerted effort from all stakeholders, including law enforcement agencies, judiciary, policymakers, and the private sector.

In conclusion, while India's legislative framework provides a foundation for addressing data theft, there is a pressing need for comprehensive reforms to bridge existing gaps and adapt to evolving threats. Proactive measures such as capacity-building, international cooperation, and public awareness campaigns are imperative to safeguarding data integrity, protecting individual rights, and fostering a secure digital ecosystem conducive to sustainable growth and development.

**REFERENCE****STATUTES**

Information Technology Act,2000

Personal Data Protection Act,2023

**ONLINE WEBSITE**

1. <https://prsindia.org/billtrack/digital-personal-data-protection-bill-2023>(last seen at 25 may 2024)
2. <https://www.lw.com/admin/upload/SiteAttachments/Indias-Digital-Personal-Data-Protection-Act2023-vs-the-GDPR-A-Comparison.pdf> (last seen at 25 may 2024)
3. <https://www.verizon.com/business/resources/articles/s/economic-impact-of-data-security-breaches-in-ecommerce/>(last seen at 28 may 2024)
4. <https://juriscentre.com/2021/05/28/law-regarding-data-theft-in-india/> (last seen at 28 may 2024)
5. <https://blog.ipleaders.in/critical-analysis-cybercrime-india/>(last seen at 30 may 2024)
6. <https://www.mondaq.com/india/data-protection/1378424/corporate-data-theft-a-major-concern>(last seen at 28 may 2024)
7. <https://www.legalserviceindia.com/article/1267-Data-Theft-in-Cyber-Space.html>(last seen at 28 may 2024);
8. <https://www.jsalaw.com/newsletters-and-updates/stringent-measures-against-cybercrimes-in-indias-new-criminal-justice-system/>(last seen at 28 may 2024)
9. [https://indraprasthalawreview.in/wp-content/uploads/2020/10/ggsipu\\_uslls\\_ILR\\_2020\\_V1-I1-13-aditi\\_palit-abhishek\\_kushwaha.pdf](https://indraprasthalawreview.in/wp-content/uploads/2020/10/ggsipu_uslls_ILR_2020_V1-I1-13-aditi_palit-abhishek_kushwaha.pdf)(last seen at 28 may 2024)

