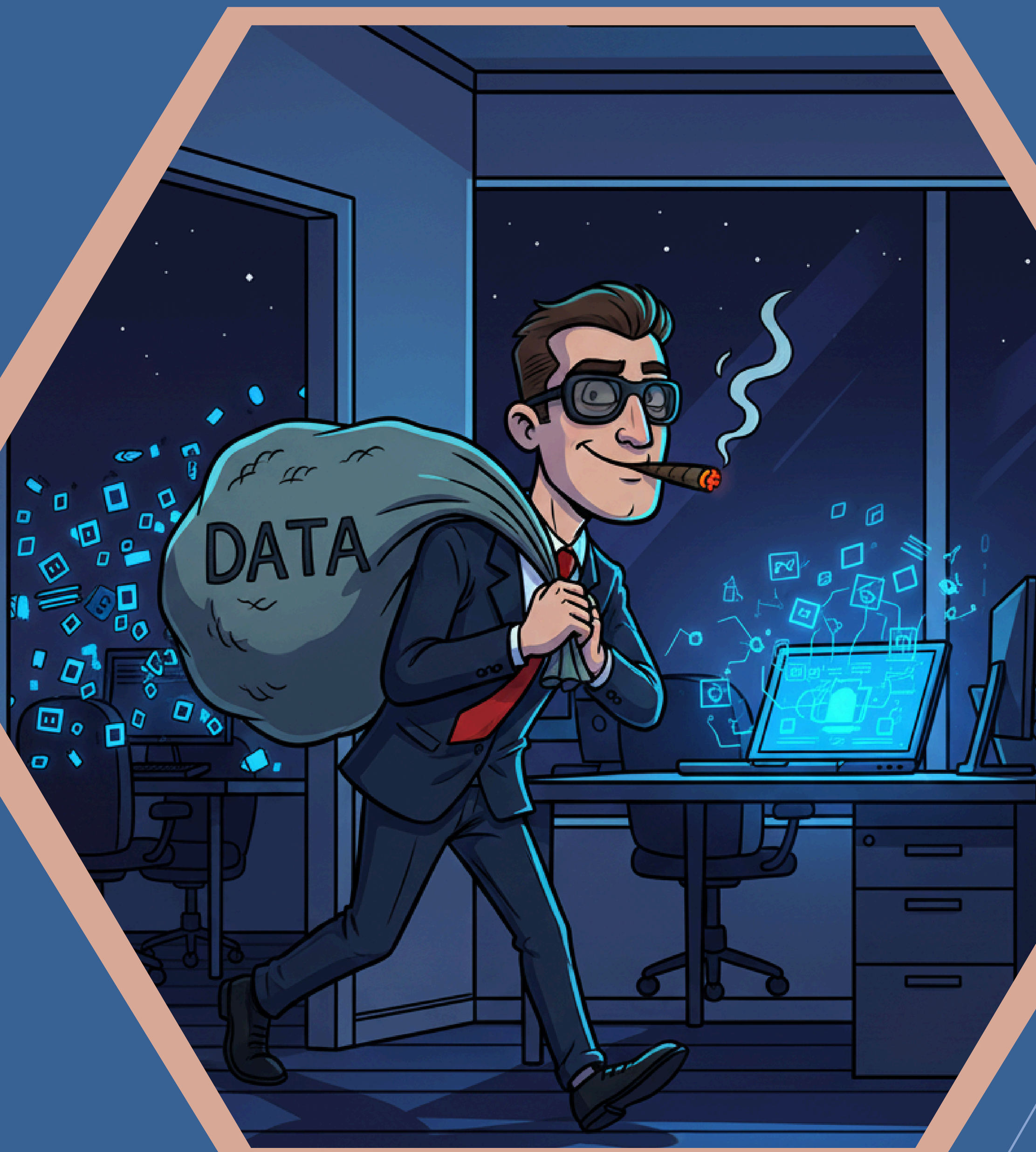
Images are generated using AI for academic purpose

YNZ GROUP

www.ynzgroup.co.in

WHISPERS IN THE SERVER ROOM: CRACKING DOWN ON WORKPLACE DATA THEFT



WEDNESDAY WISDOM

19.11.2025

I. INTRODUCTION[1]

It began with a routine resignation email on a Monday morning. A highly valued employee someone trusted with client lists, sensitive source code repositories, and years of institutional knowledge announced their departure for "better opportunities." Nothing appeared unusual. Yet, within days, managers detected irregular login attempts, missing internal files, and, soon after, the launch of a strikingly similar product by a competing firm. What seemed like an ordinary exit quietly escalated into a classic case of insider data theft, underscoring a reality of the modern workplace: in the digital era, the most significant threats to corporate security often originate not from external cybercriminals but from trusted insiders with legitimate access.

Often we hear that data is what OIL was in earlier days. The exponential growth of digital technologies, cloud computing, and remote work has made organizations increasingly vulnerable due to loss of confidential information, proprietary algorithms, client databases, and internal communications. Workplace data theft has emerged as one of the most insidious threats to corporate security. Unlike external cyberattacks, data theft by employees, contractors, or consultants betrays trust, undermines business strategy, and can cause substantial financial and reputational damage.

-
-
- The legal system has responded through a combination of statutory, contractual, and regulatory tools. In India, the **Information Technology Act, 2000**, and the **Digital Personal Data Protection Rules, 2025** have recently come into force on November 14, 2025 provide avenues for addressing these threats. However, the rapid evolution of technology has outpaced legal provisions, leading to gaps in enforcement, uncertainty in definitions, and difficulties in proving offenses. Recent judicial decisions highlight both the potential and limitations of existing legal frameworks in effectively tackling insider data theft, particularly in cases where digital data is the central "asset" in dispute.

[1] The article reflects the general work of the author on the date of publication and the views expressed are personal. No reader should act on any statement contained herein without seeking detailed professional advice.

II. Legal Framework and Challenges

Workplace data theft can manifest in various ways: unauthorized copying of databases, exfiltration of source codes, dissemination of trade secrets, or misuse of client information. The Indian legal landscape primarily addresses these issues under:

1. **Information Technology Act, 2000[2]**

a. Section 43: Penalty for damage to computer, computer system, etc. If any person without permission of the owner or any other person who is in charge of a computer, computer system or computer network

accesses or secures access to such computer, computer system or computer network	The person shall be liable to pay damages by way of compensation not exceeding Rs. 1,00,00,000/- (Rupees One Crore) to the person so affected.
downloads, copies or extracts any data, computer data base or information from such computer, computer system or computer network including information or data held or stored in any removable storage medium	
introduces or causes to be introduced any computer contaminant or computer virus into any computer, computer system or computer network; (d) damages or causes to be damaged any computer, computer system or computer network, data, computer data base or any other programmes residing in such computer, computer system or computer network;	
disrupts or causes disruption of any computer, computer system or computer network;	
Denies or causes the denial of access to any person authorised to access any computer, computer system or computer network by any means;	
provides any assistance to any person to facilitate access to a computer, computer system or computer network in contravention of the provisions of this Act, rules or regulations made thereunder;	
charges the services availed of by a person to the account of another person by tampering with or manipulating any computer, computer system, or computer network;	

[2] https://www.indiacode.nic.in/bitstream/123456789/13116/1/it_act_2000_updated.pdf

b. **Section 66:** Whoever with the intent to cause or knowing that he is likely to cause wrongful loss or damage to the public or any person destroys or deletes or alters any information residing in a computer resource or diminishes its value or utility or affects it injuriously by any means, commits hack: (2) Whoever commits hacking shall be punished with imprisonment up to three years, or with fine which may extend up to Rs. 2,00,000/- (Rupees Two lakh rupees) or with both.

c. **Section 72:** Criminalizes disclosure of confidential information obtained in electronic form.

2. Bharatiya Nyaya Sanhita (BNS)[3]

a. **Section 316(1) & 316(2):** Deal with criminal breach of trust and the corresponding punishment.

b. **BNS Section 316(4) & 316(5):** Address criminal breach of trust by clerks, servants, agents, public servants, or fiduciaries, which can extend to employees in positions of trust

3. **Contractual Remedies**

a. Non-disclosure agreements, confidentiality clauses, and restrictive covenants often supplement statutory protections, providing civil remedies for misappropriation of proprietary data.

Despite these provisions, the legal framework has notable challenges. Firstly, even though the status of digital information as 'property' under the IPC remains unsettled for purposes of offences such as theft or criminal breach of trust, judicial decisions have, in particular circumstances, recognised that the misuse of entrusted data can attract liability for criminal breach of trust. Secondly, proving insider theft is procedurally complex: linking unauthorized access to a specific employee, preserving electronic evidence integrity, and navigating digital forensics require expertise and resources that many organizations lack.

[3] https://www.mha.gov.in/sites/default/files/250883_english_01042024.pdf

III. Judicial Approaches and Landmark Judgments

Indian courts have increasingly confronted workplace data theft, especially as digital assets have become central to commercial operations. Judicial approaches reveal both an evolving understanding of the seriousness of data theft and the limitations of existing statutory provisions.

The Supreme Court's recognition of privacy as a fundamental right in **Puttaswamy v. Union of India [4]** reaffirmed the constitutional importance of data protection in the digital age. Though the judgment concerns personal data, it has indirectly influenced India's approach to regulating digital information more broadly, paving the way for statutory responses such as the DPDP Act.

In **Naveen Kumar vs State Of Karnataka (2023, Karnataka High Court)[5]**, ex-employees were accused of misappropriating client databases and violating non-disclosure agreements. The court emphasized that insider data theft constitutes a serious breach of trust and allowed criminal proceedings to continue. The judgment reinforced the applicability of both the IPC and IT Act provisions to cases involving digital information, recognizing that data can carry commercial value comparable to tangible assets.

Conversely, in the **Silicomp India case (2025, Karnataka High Court)[6]**, former employees were accused of using company data to set up a competing business. The Court emphasized that criminal proceedings should not be used for recovery of money and lack of appropriate evidence led to the quashing of the complaint.

In **Prabhat Sharma v. State of Karnataka (2025) [7]**, the Court denied anticipatory bail to employees accused of misappropriating highly sensitive defense-related data. Here, the Court underscored that the gravity of the offense particularly where national security is implicated can override procedural uncertainties or statutory ambiguities.

[4]Justice K. S. Puttaswamy (Retd.) & Anr. v. Union of India, Writ Petition (Civil) No. 494 of 2012; (2017) 10 SCC 1; AIR 2017 SC 4161

[5] 2024 Latest Caselaw 3444 (Kant); SLP (Criminal) No. 1394/2007; CRL.A No. 1993 of 2023.

[6]Ramiah Sambandam & Ors. v. State of Karnataka, Criminal Petition No. 6306 of 2024 & CRL.P No. 6295 of 2024

[7] Prabhat Sharma v. State of Karnataka (2025, KHC), CRL.P No. 695 of 2025

In this case, following the resignation of the employees, an IT audit of their laptops revealed the existence of a separate Autodesk Fusion workspace and it was alleged that the employees had illegally hacked, copied, and shared highly sensitive information including source codes and original designs.

Such cases highlight the spectrum of judicial treatment, ranging from commercial disputes to matters involving national security, and demonstrate the necessity for a nuanced legal approach to data theft.

IV. Lacunas in the Current Legal Framework

Despite the presence of statutory provisions addressing unauthorized access and misuse of digital information, certain structural and practical challenges continue to shape the treatment of workplace data-related incidents. Under the earlier IPC framework, digital information did not always align seamlessly with the definition of "movable property," leading to interpretational questions when applying traditional theft provisions. While newer legal frameworks such as the Bharatiya Nyaya Sanhita (BNS) explicitly recognize data as movable property, the transition in practical application is still ongoing. Existing statutes including the IT Act and relevant provisions under criminal law primarily address unauthorized access, downloading, or extraction of data. These provisions do not always distinguish between varying degrees of intent or between deliberate and inadvertent actions, which can result in different approaches depending on the circumstances of each case.

Investigative processes involving digital information also require specialized technical expertise. Effective inquiry into unauthorized access or data exportation depends on digital forensic capabilities and adherence to chain-of-custody standards for electronic evidence, both of which can vary across organizations and investigative bodies. In workplace settings, employee use of personal devices, encrypted platforms, or remote access tools may complicate the reconstruction of digital activity.

Multiple statutes including the IT Act, BNS provisions, and the Digital Personal Data Protection Act (DPDP Act) may apply depending on whether the information involved is personal data, proprietary business information, or both. As the DPDP Act primarily addresses personal data, workplace matters involving corporate or non-personal digital assets may continue to rely on contractual frameworks, internal policies, and general criminal or civil provisions. Courts have also noted that certain workplace data disputes may be more appropriately addressed through civil or commercial mechanisms, depending on the nature of the underlying rights and obligations.

These factors shape today's legal landscape and show why it's important to interpret laws clearly, handle electronic evidence properly, and choose the right legal process for each type of data-related incident.

V. Practical Implications and Recommendations

Given the complexities and lacunas in the legal framework, organizations must adopt a proactive, multi-layered approach to mitigate workplace data theft.

Firstly, robust internal controls such as role-based access management, audit trails, and digital monitoring systems are essential to prevent unauthorized data access. Employers should also maintain comprehensive incident response plans to secure and preserve electronic evidence in the event of a breach. In many cases, system logs can be deleted or manipulated, undermining evidentiary reliability. Employees often access sensitive information should clearly define proprietary information, obligations of departing employees, and consequences for breaches. Simultaneously, organizations should implement employee training programs to raise awareness about ethical obligations and legal liabilities associated with data misuse.

Employees, on the other hand, must understand that unauthorized use of company data even after termination can lead to civil and criminal consequences. Clear communication of policies and consistent enforcement are essential to foster a culture of compliance while protecting corporate assets. As India's digital economy continues to expand, strengthening the legal and practical mechanisms against workplace data theft is not only a matter of corporate interest but also a broader imperative for economic security and trust in the digital workplace.

For any feedback or response on this article, the authors can be reached on darshan.mundane@ynzgroup.co.in and shravani.joshi@ynzgroup.co.in

Author: Darshan Mundane

Darshan is a Legal Associate at YNZ Legal.
By qualification he is Bachelor of Legal Science and Bachelor of Law from Government Law college, Mumbai University.

Co-author: Shravani Joshi

Shravani is Legal Associate at YNZ legal.
By qualification she is Bachelor of Commerce and Bachelor of Law from Vivekanand College.