The Invisible Leak: How Everyday AI Use Is Quietly Threatening India's Data Security

By Chetan Basavraj Kharatmal | T.Y B.Sc Cybersecurity | June 2026

Every morning, millions of Indian professionals open their laptops and do something that feels entirely ordinary — they paste a work document into ChatGPT, ask Gemini to summarise a client report, or get Microsoft Copilot to draft an email from sensitive HR records. It feels productive. It feels harmless. And in many cases, it is anything but.

This is the new face of India's insider threat problem — not a rogue employee selling company secrets in the dead of night, but an ordinary person trying to do their job faster.

A Problem India Can No Longer Ignore

India is now one of the most expensive countries in the world for data breaches. According to IBM's 2025 Cost of a Data Breach Report, the average breach in India now costs organisations **₹220 million** a 13% jump from the previous year. What makes this figure more alarming is where many of these breaches originate: not from sophisticated hackers, but from within.

The rise of generative AI tools has created a blind spot in corporate security. Tools like ChatGPT, Google Gemini, and Microsoft Copilot have become as common in the Indian workplace as email. Yet 63% of Indian organisations have no formal policy on what data employees can share with these platforms. The data simply flows out payroll files, client contracts, patient records, source code typed into chat boxes by employees who genuinely believe they are just getting help with their work.

Why This Is Different From Traditional Data Theft

Traditional insider threat models assume intent. The malicious insider steals data on purpose. The systems we build to catch them monitoring USB ports, tracking large file transfers, flagging unusual email attachments are designed with that intent in mind.

But unintentional leaks through AI tools leave almost no trace. There is no file download. No suspicious login. No unusual access pattern. An HR manager who pastes a salary spreadsheet into ChatGPT to quickly identify anomalies has technically committed a data breach without ever meaning to, without any alarm going off, and often without even knowing the data may now be stored on a foreign server and potentially used for AI model training.

India's legal framework is scrambling to keep up. The Digital Personal Data Protection (DPDP) Act 2023 — a landmark piece of legislation — establishes obligations for organisations handling personal data, but it does not yet explicitly address the scenario of an employee inadvertently leaking data through a consumer AI tool. The DPDP Rules 2025, notified in November 2025, operationalise the Act further, but enforcement for AI-specific misuse remains largely uncharted.

The Human Behind the Leak

The most important word in this conversation is **unintentional**. The threat is not a hacker. It is a junior finance associate who uses ChatGPT to format a financial report. It is a healthcare receptionist who feeds patient names into an AI translation tool. It is a law student who submits internal case notes to an AI summariser for a quick revision. These people are not criminals. They are users who were never taught where the line is.

Research consistently shows that lack of awareness is the weakest link. When employees understand that public AI tools can retain their inputs, use them for training, or expose them through model vulnerabilities, their behaviour changes. But across India's tech companies, banks, hospitals, and universities, that awareness is dangerously low.

What Needs to Change

The solution is not to ban AI tools ' that ship has sailed'. Organisations need enforceable AI usage policies, not PDFs buried in onboarding packets. Security teams need to evolve beyond traditional Data Loss Prevention (DLP) systems and adopt AI-enhanced monitoring that can detect sensitive content flowing through conversational interfaces. CERT-In needs clearer guidance on AI-mediated breach reporting. And employees — technical and non-technical alike — need training that is specific, practical, and repeated.

> India is building one of the world's largest AI-powered economies. The country cannot afford to let the tools powering that future quietly drain it of its most sensitive information.

The invisible leak is real. The question is whether we will recognise it before the damage is irreversible.